Bundesnetzagentur

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Technische Richtlinie

zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV) *

Ausgabe ~~6.3~~7.0

Stand: ~~06~~xx. ~~April~~ Januar ~~2016~~2017

Bearbeiter und Herausgeber:

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
Postfach 80 01
55003 Mainz

* Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Inhaltsangabe

Inhaltsangabe.....2

1 Regelungsbereich.....5

2 Inhalt der jetzigen Ausgabe der Technischen Richtlinie.....5

3 Begriffsbestimmungen.....5

4 Normative Referenzen.....6

5 Abkürzungen.....8

Teil A Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation.....10

1 Grundsätzliches.....11
2 Aufteilung.....11
2.1 Überblick über die anlagen- bzw. dienstespezifische Anlagen und den informativen Teil.....12
3 Grundsätzliche Anforderungen.....13
3.1 Übermittlung der Überwachungskopie.....13
3.1.1 Allgemeine Anforderungen an leitungsvermittelnde Netze (PSTN und GSM).....14
3.1.2 Allgemeine Anforderungen für den Mobilfunkdienst GPRS und für UMTS.....15
3.1.3 Allgemeine Anforderungen an Speichereinrichtungen für Sprache, Fax und Daten (Voicemail-Systeme, Unified-Messaging-SystemUnified-Messaging-Systeme, ...).....15
3.1.4 Allgemeine Anforderungen für den Dienst E-Mail.....15
3.1.5 Allgemeine Anforderungen für den Internetzugangsweg.....15
3.1.6 Allgemeine Anforderungen für VoIP und sonstige Multimediadienste.....15
3.2 Richtwerte.....16
3.3 Maßnahmen zur Bereitstellung der vollständigen Überwachungskopie am IP-basierten Übergabepunkt.....17
3.3.1 Pufferung (Auslegung der bestehenden Verpflichtung).....18
3.3.2 Abstimmung der MTU-Size (Auslegung der bestehenden Verpflichtung).....18
3.3.3 „alive“-Prüfung der Verfügbarkeit der Übertragungsstrecke (neue Verpflichtung).....19
3.3.4 Standardisierte Fehlermeldungen (HI1-Messages) (neue Verpflichtung).....19
4 Sonstige Anforderungen.....20
4.1 Festlegung von Kennungen zur Umsetzung von Überwachungsmaßnahmen.....20
4.2 Übermittlungsverfahren für die Anmeldung und Bestätigung von Funktionsprüfungen der Aufzeichnungs- und Auswerteeinrichtungen der bSn.....21

Anlage A Grundsätzliche Festlegungen zur Übermittlung der Daten.....23

Anlage A.1 Festlegungen zu FTAM und FTP.....23
Anlage A.1.1 Dateiname.....23
Anlage A.1.2 Parameter.....25
Anlage A.2 Festlegungen zur Teilnahme am VPN.....28
Anlage A.3 Übermittlung von HI1- und zusätzlichen Ereignissen.....30
Anlage A.3.1 Möglichkeiten der Übermittlung.....30
Anlage A.3.2 Das nationale ASN.1-Modul 'Natparas'.....31
Anlage A.3.2.1 Übermittlung mit dem ASN.1-Modul 'HI1NotificationOperations'.....34
Anlage A.3.2.2 Implementierung im ASN.1-Modul 'HI2Operations'.....35
Anlage A.3.2.3 Implementierung im ASN.1-Modul 'Umts-HI3-PS'.....36
Anlage A.3.2.4 Übermittlung mit dem ASN.1-Parameter 'National-Parameters'.....37
Anlage A.4 Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS.....38

Anlage B Übergabepunkt für leitungsvermittelnde Netze (national).....39

Anlage B.1 Allgemeine Anforderungen.....40
Anlage B.1.1 Referenznummer und Zuordnungsnummer.....40
Anlage B.1.2 Übermittlung der Kopie der Nutzinformationen.....40
Anlage B.1.3 Übermittlung der Ereignisdaten.....41
Anlage B.1.4 Keine Übermittlung von Informationen zur TKA-V.....41
Anlage B.2 Der Datensatz.....43
Anlage B.2.1 Struktur des Datensatzes.....44
Anlage B.2.2 Parameter in den Ereignisdatensätzen.....45
Anlage B.3 Verwendung der Subadressen.....53
Anlage B.4 Dienste und Dienstmerkmale.....56

Anlage C Festlegungen für PSTN und ISDN (ETSI ES 201 671 bzw. TS 101 671)63

Anlage C.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen 64
Anlage C.2 Erläuterungen zu den ASN.1-Beschreibungen.....68

Anlage D Festlegungen für GSM, GPRS, UMTS- und LTE-Netze (3GPP TS 33.108) 69

Anlage D.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen 71
Anlage D.2 Erläuterungen zu den ASN.1-Beschreibungen.....78

Anlage E Übergabepunkt für Speichereinrichtungen für Sprache, Faksimile und Daten (Voicemail-Systeme, Unified-Messaging-Systeme etc.).....79

Anlage E.1 Begriffsbestimmungen.....79
Anlage E.2 Allgemeine Erläuterungen.....79
Anlage E.3 Grundsätzliche Ausleitungsmethoden sowie Festlegung von relevanten Ereignissen.....81
Anlage E.3.1 Grundsätzliche Ausleitungsmethoden der zu überwachenden Telekommunikation.....81
Anlage E.3.2 Grundsätzliche Festlegung von relevanten Ereignissen.....82
Anlage E.4 Anforderungen für die Überwachung von Sprach- und Faxnachrichten sowie von SMS nach Anlagen B, C oder D.....83
Anlage E.5 Anforderungen für die Überwachung von Sprach- und Faxnachrichten, SMS sowie MMS innerhalb einer XML-kodierten Datei.....85
Anlage E.5.1 Parameter der Ereignisdaten.....85
Anlage E.5.2 Die XML-Struktur und DTD für Sprache, Fax, SMS und MMS.....86

Anlage F Festlegungen für Speichereinrichtungen des Dienstes E-Mail.....91

Anlage F.1 Begriffsbestimmungen, Grundsätzliches.....91
Anlage F.2 National spezifizierter E-Mail-Übergabepunkt.....93
Anlage F.2.1 Parameter der Ereignisdaten.....95
Anlage F.2.2 XML-Struktur und DTD.....97
Anlage F.3 E-Mail-Übergabepunkt nach ETSI TS 102 232-02 (ab Version 2.1.1)....100
Anlage F.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen 100
Anlage F.3.1.1 Grundlage: ETSI TS 102 232-01 100
Anlage F.3.1.2 Grundlage: ETSI TS 102 232-02 .....103~~103~~~~102~~
Anlage F.3.2 Erläuterungen zu den ASN.1-Beschreibungen.....104~~104~~~~103~~

Anlage G Festlegungen für den Internetzugangsweg (ETSI TS 102 232-03, -04 sowie TS 101 909-20-2).....105~~105~~~~104~~

Anlage G.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen .....106~~106~~~~105~~
Anlage G.1.1 Grundlage: ETSI TS 102 232-01.....106~~106~~~~105~~
Anlage G.1.2 Grundlage: ETSI TS 102 232-03.....108~~108~~~~107~~
Anlage G.1.3 Grundlage: ETSI TS 102 232-04.....108~~108~~~~107~~
Anlage G.1.4 Grundlage ETSI TS 101 909-20-2.....109~~109~~~~108~~

Anlage G.2 Erläuterungen zu den ASN.1-Beschreibungen.....110~~110~~~~109~~

Anlage H Festlegungen für VoIP und sonstige Multimediadienste (ETSI TS 102 232-05, -06 und 101 909-20-1).....111~~111~~~~110~~

Anlage H.1 Grundsätzliche Anforderungen bei Anwendung von ´Service-specific details for IP Multimedia Services (TS 102 232-05 bzw. TS 101 909-20-1) .....112~~112~~~~111~~
Anlage H.1.1 Begriffsbestimmungen.....112~~112~~~~111~~
Anlage H.1.2 Grundsätzliches.....112~~112~~~~111~~
Anlage H.1.3 Vollständigkeit der Ereignisdaten.....112~~112~~~~111~~
Anlage H.1.4 Bereitstellung der Nutzinformationen bei getrennter Übermittlung von der Signalisierung.....113~~113~~~~112~~
Anlage H.2 Grundsätzliche Anforderungen bei Anwendung von ´Service-specific details for PSTN/ISDN services´ (ETSI TS 102 232-06).....113~~113~~~~112~~
Anlage H.3 Optionsauswahl und Festlegung ergänzender technischer Anforderungen .....114~~114~~~~113~~
Anlage H.3.1 Grundlage: ETSI TS 102 232-01.....114~~114~~~~113~~
Anlage H.3.2 Grundlage: ETSI TS 102 232-05.....118~~116~~~~115~~
Anlage H.3.3 Grundlage: ETSI TS 101 909-20-1.....120~~118~~~~117~~
Anlage H.3.4 Grundlage: ETSI TS 102 232-06.....121~~119~~~~118~~
Anlage H.4 Erläuterungen zu den ASN.1-Beschreibungen.....122~~120~~~~119~~

Teil B Technische Umsetzung gesetzlicher Maßnahmen zur Erteilung von Auskünften.....123~~121~~~~120~~

1 Grundsätzliches.....124~~122~~~~121~~
2 Übermittlungsverfahren ETSI-ESB und E-Mail-ESB.....124~~122~~~~121~~
3 Gewährleistung von Datensicherheit und Datenqualität.....125~~123~~~~122~~

Anlage A Übermittlungsverfahren ETSI-ESB.....129~~126~~~~125~~

1.1 Grundsätzliche Verfahrensbeschreibung.....129~~126~~~~125~~
1.2 Verfahrensbedingungen.....130~~127~~~~126~~
1.3 Besonderheiten der verschiedenen Verwendungsmöglichkeiten.....132~~129~~~~128~~
1.3.1 Beauskunftung von Verkehrsdaten nach § 96 und § 113b TKG (optional) .....132~~129~~~~128~~
1.3.2 Beauskunftung von Verkehrsdaten in Echtzeit (optional).....133~~130~~~~129~~
1.3.3 Beauskunftung zur Struktur von Funkzellen (optional).....133~~130~~~~129~~
1.3.4 Beauskunftung von Bestandsdaten gemäß § 113 Abs. 5 Satz 2 TKG.....133~~130~~~~129~~
1.3.5 Beauskunftung zur Standortfeststellung von mobilen Endgeräten (optional) .....134~~131~~~~130~~
1.3.6 Übermittlung der Anordnung sowie weitere Maßnahmen zur Überwachung der Telekommunikation (optional).....134~~131~~~~130~~
1.3.7 Übermittlung von Daten zum Rechnungsabgleich im Vorfeld der Entschädigung nach § 23 Absatz 1 JVEG (optional).....135~~132~~~~131~~
1.4 Elektronisch gesicherte Übermittlung der Anordnung.....135~~133~~~~131~~
2 Festlegungen für den Übergabepunkt nach der ETSI-Spezifikation TS 102 657 .....137~~134~~~~133~~
2.1 Optionsauswahl zur ETSI TS 102 657.....137~~134~~~~133~~
2.2 Ergänzende technische Anforderungen zur Schnittstellenbeschreibung der ETSI TS 102 657.....139~~136~~~~135~~
2.2.1 Übermittlungsmethode HTTP.....139~~136~~~~135~~
2.2.2 Behandlung von Fehlerfällen.....140~~137~~~~136~~
2.2.3 Festlegung zu den Formaten.....142~~139~~~~138~~
2.2.4 Normierung der Antwortdaten bei Bestands- und Verkehrsdaten-Beauskunftungen.....146~~143~~~~141~~
2.2.5 Flexible Nutzung des Freitext-Feldes „otherInformation“.....147~~144~~~~142~~
3 Definition der nationalen Parameter.....147~~144~~~~142~~
3.1 Allgemeines.....147~~144~~~~142~~
3.2 Beschreibung des nationalen XML-Moduls 'Natparas2' (für Anfragen)..148~~145~~~~143~~
3.2.1 Festlegung der Nutzungsarten.....148~~145~~~~143~~
3.2.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas2 .....149~~146~~~~144~~

3.3 Beschreibung des nationalen XML- Moduls 'Natparas3' (für Antworten) 154151149
3.3.1 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3 154151149
3.3.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3 154151149
4 Übermittlung von Rechnungsdaten bzw. Geltendmachung des Anspruchs auf Entschädigung nach § 23 Absatz 1 JVEG 158155152
4.1 Grundsätzliches 158155152
4.2 Methoden der elektronischen Übermittlung 158155152
4.3 Beschreibung des nationalen XML- Moduls 'Natparas2' (für Rechnungsdaten) 158155153
Anlage A.1 Ergänzende Erläuterungen des Verfahrens 160157154
Anlage A.1.1 Prinzipieller Kommunikationsfluss 160157154
Anlage A.1.2 Festlegungen zur Teilnahme am IP-VPN mittels Einsatz eines Kryptosystems 163160157

Anlage B Übermittlungsverfahren E-Mail-ESB 165162159

1.1 Grundsätzliche Verfahrensbeschreibung 165162159

Teil X Informativer Anhang 167164160

Anlage X.1 Geplante Änderungen der TR TKÜV 168165161
Anlage X.2 Vergabe eines Identifikationsmerkmals für bS zur Gewährleistung von eindeutigen Referenznummern 169166162
Anlage X.3 Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy) 170167163
Anlage X.4 Tabelle der anwendbaren ETSI- und 3GPP-Standards bzw. Spezifikationen sowie der ASN.1-Module 182179175
Anlage X.5 Checkliste zu den sonstigen Anforderungen nach TKÜV bei der Umsetzung von Überwachungsmaßnahmen 183180176

Fortschreibung 186183179

Ausgabenübersicht 186183179

1 Regelungsbereich

Die Technische Richtlinie (TR TKÜV) beschreibt auf der Grundlage des § 110 Abs. 3 TKG [21] i.V.m. § 11 TKÜV [14] unter Berücksichtigung der §§ 96, 113 Abs. 5 TKG technische Einzelheiten zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zur Erteilung von Auskünften.

Die TR TKÜV wird gemäß § 110 Abs. 3 TKG i.V.m. § 11 TKÜV von der Bundesnetzagentur im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände der Verpflichteten und der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen erstellt. Internationale Standards sind dabei zu berücksichtigen, Abweichungen von den Standards sind zu begründen. Die Technische Richtlinie ist von der Bundesnetzagentur auf ihrer Internetseite zu veröffentlichen; die Veröffentlichung hat die Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen.

Anpassungen der TR TKÜV an den aktuellen Stand der Technik sind von der Bundesnetzagentur im gleichen Verfahren durchzuführen.

In der TR TKÜV kann grundsätzlich festgelegt werden, bis zu welchem Zeitpunkt bisherige technische Vorschriften noch angewendet werden dürfen. In der TR TKÜV sind auch die Arten der Kennungen festzulegen, für die bei bestimmten Arten von Telekommunikationsanlagen neben den dort verwendeten Ziel- und Ursprungsadressen auf Grund der die Überwachung der Telekommunikation regelnden Gesetze zusätzliche Vorkehrungen für die technische Umsetzung von Anordnungen zu treffen sind. In Fällen, in denen neue technische Entwicklungen noch nicht in der TR TKÜV berücksichtigt sind, hat der Verpflichtete die Gestaltung seiner Überwachungseinrichtungen mit der Bundesnetzagentur abzustimmen.

2 Inhalt der jetzigen Ausgabe der Technischen Richtlinie

Die erste Ausgabe der Technischen Richtlinie erschien im Dezember 1995 als TR FÜV, Ausgabe 1.0. In den letzten 20 Jahren wurde sie fortlaufend an gesetzliche Neuregelungen und den Stand der Technik angepasst; die jetzige, 14. Ausgabe der Technischen Richtlinie erscheint als TR TKÜV, Ausgabe 6.3.

Die Ausgabe 6.3 unterscheidet sich zu ihrer Vorgängerversion, TR TKÜV, Ausgabe 6.2, hauptsächlich durch Änderungen, die infolge der Fortschreibung der bereits in der Richtlinie zur Anwendung kommenden europäischen und internationalen Standards notwendig wurden.

Die TR TKÜV, Ausgabe 6.3, beinhaltet die folgenden drei Teile A, B und X:

- **Teil A – Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation**
  In diesem Teil werden die technischen Einzelheiten der Überwachungseinrichtungen sowie die erforderlichen technischen Eigenschaften der Aufzeichnungsanschlüsse beschrieben.
- **Teil B – Technische Umsetzung gesetzlicher Maßnahmen zur Erteilung von Auskünften**
  Dieser Teil enthält die technischen Einzelheiten der Einrichtungen zur Beauskunftung von Bestands- und Verkehrsdaten sowie insbesondere das optionale Verfahren zur Übermittlung der Kopie der Anordnung zur Umsetzung von Maßnahmen.
- **Teil X – Informativer Anhang**
  Dieser informative Teil beinhaltet die geplanten weiteren Änderungen der TR TKÜV, die Grundlage der Diskussion der nächsten Ausgabe werden sollen, ergänzende Informationen zu Teil A und B dieser Ausgabe, Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA und eine Historie zu den einzelnen, bisher erschienen Ausgaben der TR TKÜV.

Die Unterschiede zur vorherigen Ausgabe 6.2 befinden sich im Teil A in den Bereichen VoIP, Mobilfunk, Internetzugang (WLAN) und der Teilnahme am VPN sowie im gesamten Teil B.

3 Begriffsbestimmungen

Ergänzend zu den Begriffsbestimmungen der TKÜV gelten zusätzlich im Sinne dieser Richtlinie folgende Begriffsbestimmungen:

3.1 Telekommunikationsinhalt (Nutzinformationen, Content of Communication, CC)

Der Anteil der zu überwachenden Telekommunikation, der die zwischen den Teilnehmern bzw. zwischen deren Endeinrichtungen ausgetauschten Nutzinformationen (z. B. Sprache, E-Mail oder IP-Verkehr) enthält.

3.2 Ereignisdaten (Intercept Related Information, IRI)

Bereitzustellende Daten gemäß § 7 TKÜV über die mit der zu überwachenden Telekommunikation zusammenhängenden näheren Umstände. Diese Daten sind auch dann bereitzustellen, wenn die Übermittlung der Telekommunikationsinhalte nicht zustande kommt (z.B. bei user busy).

3.3 Überwachungskopie

Nach § 2 Nr. 14 TKÜV das zu übermittelnde Doppel der zu überwachenden Telekommunikation (Telekommunikationsinhalt und Ereignisdaten).

3.4 Internetzugangsweg

Derjenige Übertragungsweg, der nach § 2 Nr. 12 i.V.m. § 3 Abs. 2 Nr. 3 TKÜV dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dient.

3.5 Telekommunikationsanlage-V (TKA-V)

Im Regelfall die **T**elekommuni**k**ations**a**nlage des **V**erpflichteten, in der die Telekommunikation des züA für dessen gehenden Verkehr ihren Ursprung oder für dessen kommenden Verkehr ihr Ziel hat (z. B. Teilnehmer-Vermittlungsstelle, UMS, E-Mail Server).

3.6 Transitnetz

Das Netz, über das die Überwachungskopie von der TKA-V zu der berechtigten Stelle übermittelt wird (Nutzinformationen und/oder Ereignisdaten).

3.7 Konzept

Unterlagen gemäß § 110 Abs. 1 Satz 1 Nr. 3 a TKG.

4 Normative Referenzen

Die folgende Tabelle enthält diejenigen Referenzen, die in der TR TKÜV verwendet werden:

[1]	ETS 300 007 (ITU- X.31)	Integrated Services Digital Network (ISDN); Support of packet-mode terminal equipment by an ISDN
[2]	ETS 300 011	ISDN; Primary rate user-network interface, Layer 1 specification and test principles
[3]	ETS 300 012	ISDN; Basic user-network interface, Layer 1 specification and test principles
[4]	ETS 300 090	ISDN; Calling line identification restriction (CLIR) supplementary service; Service description
[5]	ETS 300 094	ISDN; Connected line identification presentation (COLP) supplementary service; Service description
[6]	EN 300 403-1	ISDN; Benutzer-Netz-Schnittstelle Schicht 3, Spezifikation für Basisabläufe der Verbindungssteuerung
[7]	ETS 300 108	ISDN; Circuit-mode 64 Kbit/s unrestricted 8 kHz structured bearer service category; Service description

[8]	ETS 300 133-X	Paging Systems (PS); European Radio Message System (ERMES) Parts 1 - 4
[9]	ETS 300 136	ISDN; Closed User Group (CUG) supplementary service; Service description
[10]	ETS 300 383	ISDN; File transfer over the ISDN EUROFILE transfer profile
[11]	ETS 300 409	ISDN; Eurofile transfer teleservice; Service description
[12]	ETS 300 485	ISDN; Use of cause and location in DSS1 and ISUP (ITU-T Rec. Q.850 (1993, modified)
[13]	ETS 300 523	European digital cellular telecommunications system (Phase 2); Numbering, addressing and identification (GSM 03.03)
[14]	TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)
[15]	ISO/IEC 8571	File Transfer, Access and Management
[16]	ISO/IEC ISP 10607-1	File Transfer, Access and Management; Part 1: Specification of ACSE, Presentation and Session Protocols for the use of FTAM
[17]	ISO/IEC ISP 10607-3	File Transfer, Access and Management; Part 3: Simple File Transfer Service (unstructured)
[18]	ITU-T G.711	Pulse Code Modulation (PCM) of Voice Frequencies
[19]	ITU-T H.221	Line Transmission of non-Telephone Signals; Frame Structure for a 64 to 1920 Kbit/s Channel in audiovisual Teleservices
[20]	ITU-T X.25	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit
[21]	TKG	Telekommunikationsgesetz
[22]	ES 201 671/ TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
[23]	TS 133 108	Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)
[24]	RFC 822	Standard for the Format of ARPA Internet Text Messages
[25]	RFC 2822	Internet Message Format
[26]	RFC 2045	Multipurpose Internet Mail Extensions, (MIME) - Format of Internet Message Bodies
[27]	RFC 2060	Internet Message Access Protocol - Version 4rev1
[28]	RFC 3261	SIP: Session Initiation Protocol. June 2002.
[29]	TS 102 232 bzw. TS 102 232-01	Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery
[30]	TS 102 233 bzw. TS 102 232-02	Telecommunications security; Lawful Interception (LI); Service specific details for E-mail services
[31]	TS 102 234 bzw. TS 102 232-03	Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services
[32]	TS 102 815 bzw. TS 102 232-04	Telecommunications security; Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception
[33]	TS 101 909-20-2	Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services
[34]	TS 102 232-05	Telecommunications security; Lawful Interception (LI); Service specific details for IP Multimedia Services

[35]	TS 102 232-06	Telecommunications security; Lawful Interception (LI); Service specific details for PSTN/ISDN services
[36]	TS 101 909-20-1	Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services
[37]	TS 102 657	Telecommunications security; Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data

5 Abkürzungen

Innerhalb der TR TKÜV werden folgende Abkürzungen verwendet:

ASCII	American National Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
BA	ISDN-Basisanschluss
BC	Bearer Capability
BMWi	Bundesministerium für Wirtschaft und Energie
bS, bSn	berechtigte Stelle, berechtigte Stellen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Base Station Subsystem
CC	Content of Communication
CLIP/R	Calling Line Identification Presentation / Restriction
COLP/R	Connected Line Identification Presentation / Restriction
CUG	Closed User Group
DCF77	Zeitzeichensender ‘Mainflingen’ auf der Frequenz 77,5 kHz, über den die von der PTB erzeugte amtliche Zeit für die Bundesrepublik Deutschland ausgestrahlt wird
DCS	Digital Cellular System
DDI	Direct Dialing In
DM	Dienstmerkmal
DSS1	Digital Subscriber Signalling System Nr. 1
DTD	Document Type Definition
ERMES	European Radio Message System
ESB	Spezifikation der elektronischen Schnittstelle für Auskunfts- und Verbindungsdatenersuchen sowie Telekommunikationsüberwachungen und Ortungen
ETSI	European Telecommunications Standards Institute
FTAM	File Transfer, Access and Management
FTP	File Transfer Protocol
GLIC	GPRS Lawful Interception Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HI	Handover Interface
HLC	High Layer Compatibility
IMAP	Internet Message Access Protocol
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligentes Netz
IP	Internet Protocol
IPS	Internet Protocol Stack
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agencies

LI	Lawful Interception
LLC	Low Layer Compatibility
LTE	Long Term Evolution
LTMP	Local Mail Transfer Protocol
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
NEID	Network Element Identifier
OID	Object Identifier
PMXA	ISDN-Primärmultiplexanschluss
POP3	Post Office Protocol 3
PSTN	Public Switched Telephone Network (analoges Telefonnetz oder analoge Anschlüsse an digitalen Netzknoten)
PTB	Physikalisch-Technische Bundesanstalt
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SUB	SUBaddressing (supplementary service)
TCP	Transport Control Protocol
TFTS	Terrestrial Flight Telecommunication System
TKA-V	Telekommunikationsanlage des Verpflichteten
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
UDI	Unrestricted digital information
UMS	Unified-Messaging-System
UMTS	Universal Mobile Telecommunications System
UPT	Universal Personal Telecommunication
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
UTM	Universale Transversale Mercator-Projektion (Koordinatenangabe)
VoIP	Voice over IP
VMS	Voice Mail System
VPN	Virtual Private Network
WGS	World Geographic System
XML	Extensible Markup Language
ZGS	Zeichengabesystem
züA	zu überwachender Anschluss oder zu überwachende Kennung

Teil A

Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation

1 Grundsätzliches

Dieser Teil A der Technischen Richtlinie (TR TKÜV) beschreibt auf der Grundlage des § 110 Abs. 3 TKG [21] i.V.m. § 11 TKÜV [14] die technischen Einzelheiten der Überwachungseinrichtungen sowie die erforderlichen technischen Eigenschaften der Aufzeichnungsanschlüsse.

Schließlich werden auch die Arten der Kennungen festgelegt, für die bei bestimmten Arten von Telekommunikationsanlagen neben den dort verwendeten Ziel- und Ursprungsadressen auf Grund der die Überwachung der Telekommunikation regelnden Gesetze zusätzliche Vorkehrungen für die technische Umsetzung von Überwachungsmaßnahmen zu treffen sind.

In Fällen, in denen technische Entwicklungen noch nicht in der TR TKÜV berücksichtigt sind, hat der Verpflichtete die Gestaltung seiner Überwachungseinrichtungen mit der Bundesnetzagentur abzustimmen.

2 Aufteilung

Die Aufteilung des Teils A in die folgenden Abschnitte dient der möglichst einfachen Zuordnung der technischen Anforderung zu den verschiedenen Telekommunikationsanlagen oder -diensten. Hierzu sind die anlagen- bzw. dienstespezifischen Anforderungen (z.B. an ISDN-Netze, Internetzugangswege, oder Server für den Dienst E-Mail) in getrennten Anlagen beschrieben, die zusammen mit den grundsätzlichen und sonstigen Anforderungen als eigenständige Beschreibung der Anforderung zu einem konkreten Übergabepunkt nutzbar sind:

- **Grundsätzliche Anforderungen**
  Diese Anforderungen gelten für alle Übergabepunkte gleichermaßen und sind in den Kapiteln 5 und 6 dargestellt.
- **Sonstige Anforderungen**
  Nach Bedarf können die neben der Beschreibung der technischen Anforderungen zu den Übergabepunkten in § 11 TKÜV genannten, sonstigen Regelungsbereiche in der TR TKÜV aufgenommen werden. Diese sind in Kapitel 6 enthalten.
- **Anlagen- bzw. dienstespezifische Anforderungen**
  Die genauen Anforderungen zur Gestaltung der anlagen- bzw. dienstespezifischen Übergabepunkte sind in den entsprechenden Anlagen enthalten. Anlage A enthält Festlegungen zu den möglichen Übermittlungsmethoden.

2.1 Überblick über die anlagen- bzw. dienstespezifische Anlagen und den informativen Teil

Dieser Teil der TR TKÜV beschreibt den Übergabepunkt für leitungsvermittelnde Netze (Festnetze und Mobilfunknetze) sowie für VoIP und sonstige Multimediadienste, für GPRS, UMTS, UMS, E-Mail und für den Internetzugangsweg.

Die Beschreibung des jeweiligen Übergabepunktes erfolgt in folgenden Anlagen der TR TKÜV:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter)
Anlage A.2	Teilnahme am VPN mittels Kryptobox
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlicher Ereignisse
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage B	Übergabepunkt für leitungsvermittelnde Netze (PSTN, ISDN und GSM). Diese nationale Festlegung erfolgte vor der Aufnahme eines entsprechenden ETSI-Standards und kann nur noch für Erweiterungen bestehender leitungsvermittelnder Netze verwendet werden. Für neue leitungsvermittelnde Netze gelten die Beschreibungen nach Anlage C.
Anlage C	Festlegungen für **leitungsvermittelnde Fest- und Mobilfunknetze** (PSTN und GSM) **und für GPRS** nach dem ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 [22].
Anlage D	Festlegungen für **UMTS-Netze** nach der 3GPP-Spezifikation TS 33.108 [23].
Anlage E	Festlegungen für **Speichereinrichtungen** (**UMS**, **VMS** etc.) für Sprache, Fax, SMS, MMS etc. Da in den Festlegungen nach den Anlagen A bis D derartige Systeme nicht berücksichtigt sind, müssen diese Anforderungen ggf. zusätzlich erfüllt werden.
Anlage F	Festlegungen für den Dienst **E-Mail** nach nationalen Anforderungen oder der ETSI-Spezifikation **TS 102 232-02** [30]
Anlage G	Festlegungen für den **unmittelbaren teilnehmerbezogenen Zugang zum Internet** nach den ETSI-Spezifikationen TS 102 232-03 [31], TS 102 232-04 [32] oder TS 101 909-20-2 [33]
Anlage H	Festlegungen für VoIP und Multimediadienste, die auf SIP, RTP bzw. H.323 und H.248 sowie für emulierte PSTN/ISDN-Dienste nach ETSI-Spezifikationen TS 102 232-05 [34], TS 102 232-06 [35] sowie TS 101 909-20-1 [36]

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

3 Grundsätzliche Anforderungen

Diese Technische Richtlinie legt die technischen Einzelheiten fest, die zur Sicherstellung einer vollständigen Erfassung der zu überwachenden Telekommunikation und zur Gestaltung des Übergabepunktes zu den bSn erforderlich sind.

Zusätzlich sind die Anforderungen zu beachten, die sich unmittelbar aus den Vorschriften der TKÜV ergeben.

3.1 Übermittlung der Überwachungskopie

Die zu überwachende Telekommunikation setzt sich aus Nutzinformationen und Ereignisdaten zusammen.

Die Telekommunikation ist grundsätzlich auch dann zu überwachen, wenn diese zu einer anderen Zieladresse um- oder weitergeleitet wird.

> *Anmerkung:*
> *Beispielsweise gilt diese Forderung bei Telefondienstmerkmalen wie Call Forwarding oder Call Deflection, bei denen die Verbindung vom Netz oder vom Terminal des züA weitergeschaltet wird. Hier muss die Überwachungskopie zur bS übermittelt werden, solange die weitergeschaltete Verbindung besteht. Ebenso müssen auch E-Mail-Nachrichten überwacht werden, die automatisiert zu einer anderen E-Mail-Adresse eines anderen E-Mail-Postfachs weitergeleitet werden*
> *Sofern die Übergabe einer bereits zustande gekommenen Telekommunikation im Einzelfall durch den züA veranlasst wird (z. B. mittels Explicit Call Transfer (ECT)), muss die Übermittlung der Kopie der Telekommunikation zur bS eingestellt werden, sobald die Verbindung zwischen Netz und züA ausgelöst ist.*

Die Ereignisdaten müssen zeitnah, d. h. unverzüglich nach Auftreten des entsprechenden Ereignisses (z. B. Aufrufen, Löschen oder Aktivieren eines Dienstes oder Dienstmerkmals, Nutzung eines Dienstmerkmals zur Datenübertragung) erzeugt und an die bS gesendet werden. Ggf. können mehrere gleichartige Ereignisse (z. B. bei sequentieller Wahl) zusammengefasst und dann in einem Datensatz übertragen werden. Insbesondere ist bei Beginn und Ende der zu überwachenden Telekommunikation sowie bei jedem Ereignis während der Telekommunikation (z. B. Aktivitäten im Rahmen eines Dienstmerkmals) ein Ereignisdatensatz zu übermitteln, der die relevanten Daten enthält.

Zu den Ereignissen gehören auch Registrier-/Aktivierungsvorgänge von Dienstmerkmalen, soweit die Steuerung solcher Betriebsmöglichkeiten auf direktem Weg (z. B. mittels des Telefonanschlusses des züA) oder auf indirektem Weg (z.B. mittels eines anderen Telefonanschlusses über eine Service-Rufnummer oder per Webzugang) stattfindet.

Zusätzlich zum Normalfall, d. h. Übermittlung der Nutzinformationen mit zeitnaher Übermittlung der Ereignisdaten, muss es auf Anforderung der bS möglich sein, für eine bestimmte Überwachungsmaßnahme nur die Ereignisdaten, nicht jedoch die Kopie der zugehörigen Nutzinformationen, zur bS zu übermitteln. In diesem Fall sind z. B. bei der Überwachung leitungsvermittelter Telekommunikation keine ISDN-Verbindungen zur bS aufzubauen.

Die Verbindungen zur Übermittlung der Überwachungskopie sind unmittelbar nach erfolgreicher Übermittlung auszulösen, d. h. der Zugang zur bS darf nicht unnötig lange belegt werden.

Bei der Übermittlung sind die Nutzinformationen und die zugehörigen Ereignisdaten so zu kennzeichnen, dass sie einander eindeutig zugeordnet werden können (§ 7 Abs. 2 TKÜV). Hierzu erhält jede Überwachungsmaßnahme eine Referenznummer. Zusätzlich müssen die einzelnen Verbindungen innerhalb einer Überwachungsmaßnahme mit einer für die jeweilige Verbindung eindeutigen Zuordnungsnummer versehen werden.

Treten Hindernisse bei der Übermittlung der Überwachungskopie auf, müssen zumindest die Ereignisdaten nachträglich übermittelt werden (Anlage A.4).

3.1.1 Allgemeine Anforderungen an leitungsvermittelnde Netze (PSTN und GSM)

Die Anforderungen zur Gestaltung des Übergabepunktes richten sich grundsätzlich nach Anlage C und beziehen sich auf den ETSI-Standard **ES 201 671** bzw. die ETSI-Spezifikation **TS 101 671** [22].

Für bereits vor dem 01.01.2005 in Betrieb genommene leitungsvermittelnde Netze kann der Übergabepunkt jedoch weiterhin nach den nationalen Festlegungen der Anlage B gestaltet werden; dies gilt auch für Erweiterungen bestehender leitungsvermittelnder Netze.

Für die Übermittlung der Kopie der Nutzinformationen ist in beiden Möglichkeiten die Nutzung von Wählverbindungen vorgesehen.

Nach Anlage B werden die Ereignisdaten in einer ASCII-kodierten Datei per FTAM über das X.25/X.31-Netz übermittelt; nach Anlage C in einer ASN.1-kodierten Datei per FTP über das Internet.

- Die nachfolgenden besonderen Anforderungen gelten gleichermaßen bei der Realisierung nach Anlage B und Anlage C: Zur Übermittlung der Kopie der Nutzinformation werden von der TKA-V zwei transparente Wählverbindungen (Circuit-mode 64 kbit/s unrestricted, ETS 300 108 [7]) zur bS aufgebaut, unabhängig von dem Dienst, den der züA bzw. dessen Telekommunikationspartner beim Verbindungsaufbau anfordert, von denen eine die Kopie der vom züA gesendeten Nutzinformationen und die andere die Kopie der für den züA bestimmten Nutzinformationen zu den technischen Einrichtungen der bS überträgt. Die Übermittlung der Kopie der Nutzinformationen zur bS erfolgt somit richtungsgetrennt.

  Anmerkung: Bei der Nutzung des Dienstmerkmals ´Große Konferenz (CONF)´ enthalten die für den züA bestimmten Nutzinformationen die gesendeten Nutzinformationen aller anderen Teilnehmer (Summensignal). Die Kopie der vom züA ausgehenden Telekommunikation (Einzelsignal des züA) ist über die zweite Verbindung zur bS zu übertragen.

- Ist die Nutzinformation des züA Sprache, so muss diese der bS entsprechend ITU-T-Empfehlung G.711 A-law, angeboten werden. Netzseitige Kodierungen sind zu entfernen.

  Anmerkung 1: Wird z. B. die Sprachinformation in der TKA-V nach anderen Verfahren (z. B. im GSM nach 'Half rate speech transcoding') übermittelt oder werden Komprimierverfahren zur Mehrfachausnutzung der Kanäle angewendet, so muss diese Sprachinformation für die bS von der TKA-V auf das Kodierverfahren nach ITU-T-Empfehlung G.711, A-law [18], überführt werden.

  Anmerkung 2: Sprachübertragung ist nicht nur im (3,1-kHz-)Telefondienst möglich, sondern auch in anderen Diensten, z. B. im Bildtelefondienst und 7-kHz-Telefondienst. Dabei wird von den Endeinrichtungen der Benutzer im 64-kBit/s-B-Kanal bzw. in den B-Kanälen ein Rahmen (z. B. nach ITU-T-Empfehlung H.221 [19]) aufgebaut und mit entsprechenden Informationen (Sprache, Bild, Daten) belegt. Diese Nutzinformationen werden nicht von der TKA-V dekodiert, sondern von den technischen Einrichtungen der bS.

- Grundsätzlich müssen die Verbindungen zur Übermittlung der Kopie der Nutzinformationen von der TKA-V jeweils unmittelbar nach dem Erkennen des Beginns der zu überwachenden Telekommunikation, d. h. quasi zeitgleich mit dem Aufbau der Verbindung von oder zum züA zu den Anschlüssen der jeweiligen bS aufgebaut und unmittelbar nach dem Erkennen des Endes der zu überwachenden Telekommunikation ausgelöst werden.

  Anmerkung: Beispielsweise ist der Beginn einer ISDN-Verbindung demnach nicht der Zeitpunkt, zu dem der gerufene Anschluss antwortet und der Nutzkanal durchgeschaltet wird, sondern bereits der Zeitpunkt des Beginns der Signalisierung (bei gehenden Verbindungen im ISDN oder GSM der Empfang der SETUP-Nachricht bei der TKA-V, im PSTN der Schleifenschluss in der Anschlussleitung). Nur dadurch, dass die Verbindung zur bS frühzeitig mit der ersten Signalisierung aufgebaut wird, kann verhindert werden, dass Teile der Nutzinformation am Anfang der Verbindung verloren gehen.

- Der Verbindungsaufbau vom züA zu dessen Telekommunikationspartner bzw. umgekehrt darf nicht verzögert werden, auch dann nicht, wenn sich der Aufbau der Verbindung zur bS verzögert (z. B. durch Wiederholung des Verbindungsaufbauversuches).

- Die Anschlüsse der TKA-V, über die die Überwachungskopie an die bS übermittelt wird, dürfen auf der Seite des Verpflichteten nur für gehende Verbindungen eingerichtet sein. Um die Übermittlung der Überwachungskopie jederzeit zu gewährleisten, dürfen die Anschlüsse der bSn nur kommend betrieben werden.

- Die Anschlüsse der bS müssen entsprechend der Technologie gestaltet sein, die für die Übermittlung der Überwachungskopie genutzt wird. Soweit es die Art der zu überwachenden Telekommunikation technisch erlaubt, ist die zu überwachende Telekommunikation (Nutzinformationen und Ereignisdaten) zu den bei den bSn vorhandenen EURO-ISDN-Primärmultiplexanschlüssen (PMXA) oder EURO-ISDN-Basisanschlüssen (BA) nach ETS 300 012 [3] zu leiten. Darüber hinaus werden bei der bS automatisch antwortende Einrichtungen angeschaltet, so dass für diese Verbindungen die Rufphase entfällt.

- Die Verbindungen zur Übermittlung der Kopie der zu überwachenden Telekommunikation zu der jeweiligen bS werden jeweils bei Bedarf von der TKA-V aufgebaut. Die Initiative für den Verbindungsaufbau geht von der TKA-V aus. Sollte der Aufbau der leitungsvermittelten Verbindung(en) zur Übermittlung der Nutzinformationen zur bS erfolglos bleiben, erfolgen drei weitere Verbindungsaufbauversuche im Abstand von je 5 bis 10 Sekunden.

3.1.2 Allgemeine Anforderungen für den Mobilfunkdienst GPRS und für UMTS

Die Anforderungen zur Gestaltung des Übergabepunktes bezüglich GPRS können wahlweise entsprechend Anlage C nach ETSI-Standard ES 201 671 bzw. die ETSI-Spezifikation TS 101 671 [22] oder auf der Grundlage von Anlage D nach der 3GPP-Spezifikation TS 33.108 [23] gestaltet werden.

Die Regelungen bezüglich der Multimedia Domain für UMTS sind ausschließlich in der Anlage D enthalten.

3.1.3 Allgemeine Anforderungen an Speichereinrichtungen für Sprache, Fax und Daten (Voicemail-Systeme, Unified-Messaging-SystemUnified-Messaging-Systeme, ...)

Bietet der Verpflichtete seinen Kunden die Möglichkeit, Nachrichten in Sprachspeicher- oder vergleichbaren Speicher-Einrichtungen zu hinterlegen, die dem züA zugeordnet sind, ist jeweils eine Kopie einer dort eingehenden und der von dort abgerufenen Nachricht einschließlich der entsprechenden Ereignisdaten an die bS zu übermitteln. Änderungen der Einstellungen, wie das Erstellen von Versandlisten sind ebenfalls zu berichten.

Die Übermittlung der Kopie der Nutzinformationen aus diesen Speichereinrichtungen zur bS erfolgt im Regelfall zur gleichen Zielrufnummer wie die Kopie der Nutzinformationen, die vom züA herrühren oder für diesen bestimmt sind. Soweit es die technischen Einrichtungen der TKA-V erlauben, muss es der bS technisch möglich sein, die Kopie der Nutzinformationen aus derartigen Speichereinrichtungen für eine individuelle Überwachungsmaßnahme auf Verlangen der bS an eine andere Zielrufnummer zu adressieren.

Die technischen Details des Übergabepunktes enthält Anlage E.

3.1.4 Allgemeine Anforderungen für den Dienst E-Mail

Die Anlage F enthält zwei alternative Beschreibungen eines Übergabepunktes zur Überwachung des Dienstes E-Mail:

- national festgelegter Übergabepunkt nach Anlage F.2
- Übergabepunkt entsprechend ETSI-Spezifikation TS 102 232-02 [30] nach Anlage F.3.

3.1.5 Allgemeine Anforderungen für den Internetzugangsweg

Nach § 3 TKÜV sind Betreiber von Übertragungswegen, die dem unmittelbaren teilnehmerbezogenen Internetzugang dienen (z.B. Internetzugangsweg über xDSL, CATV, WLAN), verpflichtet, Vorkehrungen zur Überwachung des gesamten IP-Verkehrs zu treffen.

Hierzu enthält Anlage G drei verschiedene auf ETSI-Spezifikationen basierende Alternativen für die Ausleitung des zu überwachenden IP-Verkehrs auf Layer 2- oder Layer 3-Ebene sowie auf Basis der IP-Cablecom-Architektur.

3.1.6 Allgemeine Anforderungen für VoIP und sonstige Multimediadienste

Die Anlage H bezieht sich auf Dienste, die auf dem Session Initiation Protocol (SIP) und dem Realtime Transport Protocol (RTP) oder auf den ITU-T Standards H.323 und H.248 beruhen und bietet zudem sog. emulierten PSTN/ISDN-Diensten die Möglichkeit, die Kopie des Telekommunikationsinhaltes über RTP anstatt über ISDN-Wählverbindungen zu übermitteln.

Darüber hinaus bezieht sich die Anlage auf solche Multimediadienste, die mittels der IP-Cablecom-Architektur erbracht werden.

3.2 Richtwerte

Nach § 5 Abs. 6 TKÜV gilt grundsätzlich, dass die Dimensionierung des Administrierungssystems sowie der Kapazitäten zur Ausleitung der Überwachungskopien zur bS je nach Anzahl der umzusetzenden Überwachungsmaßnahmen bedarfsgerecht erfolgen muss.

Die Erfüllung dieser Anforderung setzt regelmäßig ein Monitoring der vorgehaltenen Überwachungs- und Ausleitungskapazität (Interceptionpoint bis Internetübergabepunkt) voraus, insbesondere bei bandbreitenbasierten Angeboten. Bei einer hohen Abweichung des durchschnittlichen Bandbreitenbedarfs eines Anschlusses zu der maximal verfügbaren Bandbreite muss eine grundsätzlich höhere Auslastung der zu überwachenden Anschlüsse berücksichtigt werden.

Die diesbezüglichen technischen und organisatorischen Vorkehrungen müssen nach Maßgabe des
§ 19 Abs. 2 Nr. 5 TKÜV im Konzept beschrieben werden.

Auf der Grundlage statistischer Erhebungen wird als Erst-Dimensionierung für den leitungsvermittelnden Bereich als Planungshilfe empfohlen, dass nach den nachstehenden Annahmen mindestens

1. die Anzahl **M** an unabhängigen Überwachungsmaßnahmen gleichzeitig eingerichtet und
2. davon mindestens für die Anzahl **A** an Überwachungskopien gleichzeitig zu den bSn übermittelt werden kann.

Darüber hinaus muss ein Mehrbedarf rechtzeitig erkannt (z.B. wenn dauerhaft eine bestimmte Auslastung erreicht wird) und das System entsprechend erweitert werden.

Es gilt folgender Zusammenhang:

$$M = a * x^{0,45}$$

$$A = V * M$$

Dabei sind:

M = Anzahl der aktivierbaren Überwachungsmaßnahmen

a = Anlagenspezifischer Faktor

x = Anzahl der potentiellen züA

A = Anzahl der gleichzeitig übermittelbaren Überwachungskopien

V = Faktor, der den Verkehrswert der jeweiligen Telekommunikationsanschlüsse berücksichtigt

Für verschiedene Arten von TK-Anlagen gelten folgende Annahmen:

a) für leitungsvermittelnde Festnetze (ISDN/PSTN) sowie Anlagen für VoIP und andere Multimediadienste:

   a = 0,75

   x = Gesamtzahl der Beschaltungseinheiten BE (z.B. analoger Teilnehmeranschluss oder ein B-Kanal eines ISDN-Basis- oder -Primärmultiplexanschlusses) in einem Netzknoten.

V = Als Verkehrswert für überwachte Anschlüsse wird der dreifache Verkehrswert einer gewöhnlichen BE in einem Netzknoten während der Hauptverkehrsstunde empfohlen.

Die Formel ist auf jeden Netzknoten separat anzuwenden.

b) für leitungsvermittelnde Dienste in Mobilfunknetzen (GSM und UMTS-CS):

a = 0,75

x = Gesamtzahl der Mobilfunkanschlüsse, die leitungsvermittelnde Dienste unterstützen.

V = Als Verkehrswert für überwachte Anschlüsse wird der dreifache Verkehrswert eines gewöhnlichen Mobilfunkanschlusses während der Hauptverkehrsstunde empfohlen.

Zusatz für die Umsetzung sog. Auslandskopf-Überwachungen nach § 4 Abs. 2 TKÜV:

Systembedingt ist die Kapazität der Administrierung von Maßnahmen bei älteren ISDN-Vermittlungs-stellen limitiert; zudem können regelmäßig weniger Ausleitungsziele als Maßnahmen administriert werden (z.B. im Festnetz lediglich 255 Ausleitungsziele für 1.024 Maßnahmen).
Um im Festnetz seitens einer bS mehrere Maßnahmen auf dem gleichen Ausleitungsziel empfangen und zuordnen zu können, muss die Zuordnung über die Subadresse nach Anlage B.3.2 erfolgen, in der derzeit die bekannte ausländische Rufnummer enthalten ist. Da dies bei Mehrfachüberwachungen für das gleiche Ausleitungsziel nicht möglich ist, muss mittelfristig die Angabe einer angepassten Referenznummer in der Subadresse nach Anlage B.3.3 erfolgen.

Beispiel für eine Vermittlungsstelle nach Buchstabe a)

a = 0,75
x = 5.000 Basis ISDN-Anschlüsse = 10.000 B-Kanäle

$M = 0,75 * 10.000^{0,45}$
M = 47 gleichzeitig aktivierbare Maßnahmen

V = 0,24 wenn der durchschnittliche Verkehrswert 0,08 beträgt

*A = 0,24 * 47*
A = 11 gleichzeitig auszuleitende ISDN-Basis-Anschlüsse (je zwei ISDN-Stiche zur bS)

3.3 Maßnahmen zur Bereitstellung der vollständigen Überwachungskopie am IP-basierten Übergabepunkt

Der Verpflichtete hat der berechtigten Stelle gemäß § 5 Abs. 2 TKÜV am Übergabepunkt eine vollständige Kopie der Telekommunikation bereitzustellen. Gemäß § 8 Abs. 2 ist die Anlage so zu gestalten, dass die Qualität der am Übergabepunkt bereitgestellten Überwachungskopie grundsätzlich nicht schlechter ist als die der zu überwachenden Telekommunikation. Neben der Kopie der Telekommunikation hat der Verpflichtete am Übergabepunkt auch die Ereignisdaten bereitzustellen (§ 7 TKÜV).

Der Verpflichtete hat durch geeignete Vorkehrungen sicherzustellen, dass die Vollständigkeit der genannten Daten

- am Erfassungspunkt der Kopie der Telekommunikation sowie der Ereignisdaten,
- auf dem Übertragungsweg zum Übergabepunkt (Delivery Function) sowie
- am Übergabepunkt

gewährleistet ist (**z.B. durch ausreichende Übertragungskapazität, Redundanzen, netzwerktypische Puffermechanismen, Wahl des Übertragungsverfahrens,**

Monitoring der Übertragungsstrecke, Loadbalancing am Eingang der Delivery Function, Abstimmung der MTU-Size).

(Als Delivery Function wird hier die technische Einrichtung bezeichnet, welche die netzinternen Daten entgegennimmt, aufbereitet und am Übergabepunkt bereitstellt.)

Für den Fall, dass die Übermittlung der Daten vom Erfassungs- zum Übergabepunkt ausnahmsweise nicht möglich ist, hat der Verpflichtete die Ereignisdaten unverzüglich nachträglich zu übermitteln, so wie es nach § 10 TKÜV auch für die Übermittlung der Daten vom Übergabepunkt an den Aufzeichnungsanschluss vorgesehen ist. Sofern es das auf der Strecke genutzte Übertragungsprotokoll (z.B. TCP) zulässt, ist für die Kopie der Telekommunikation eine zumindest kurzzeitige Pufferung am Erfassungspunkt vorzusehen, die sich an der Verfügbarkeit und der Auslastung der Übertragungsstrecke vom Erfassungspunkt bis zum Eingang der Delivery Function orientiert. Ist eine Pufferung nicht möglich (z.B. bei Nutzung von UDP) ist die Übertragungsstrecke so zu gestalten (z.B. durch ausreichende Dimensionierung, Redundanzen), dass Lastspitzen nicht zum Verlust von Daten führen.

Die ausreichende Dimensionierung der Eingangsbandbreite der Delivery Function ist gegeben, wenn der durchschnittliche, innerhalb 24 Stunden gemessene Datenstrom 60% der maximalen Eingangsbandbreite nicht überschreitet. Zudem darf die zur Verfügung stehende Eingangsbandbreite den dreifachen Wert des Kundenanschlusses mit der höchsten Bandbreite nicht unterschreiten. Damit soll gewährleistet werden, dass ein kurzfristiger Anstieg der Bandbreite durch starke Nutzung eines überwachten Anschlusses nicht zu Datenverlusten führt.

Erfolgt die Vervielfachung von Daten im Falle einer Mehrfachausleitung in der Delivery Function, so ist der entsprechende Mehrbedarf an Verarbeitungs- und Übertragungskapazität bei der Dimensionierung zu berücksichtigen. Andernfalls ist die Mehrfachausleitung im Erfassungspunkt zu realisieren.

Der Übergabepunkt ist gemäß § 8 Abs. 1 TKÜV in der TR TKÜV definiert. Die Bereitstellung der Kopie der Telekommunikation sowie der Ereignisdaten erfolgt bei einem TCP/IP-basierten Übergabepunkt über einen VPN-gesicherten Übertragungsweg an die Aufzeichnungsanschlüsse der bSn. Zur Sicherstellung dieser TCP/IP-basierten Übertragung müssen mindestens die nachfolgend genannten Vorkehrungen eingehalten werden, die sich auf Ausleitungen nach den Anlagen D, G und H beziehen (die Übermittlung von IRI per FTP ist von diesen Vorkehrungen nicht betroffen).

3.3.1 Pufferung ~~(Auslegung der bestehenden Verpflichtung)~~

Ist die Übermittlung der Überwachungskopie an den Aufzeichnungsanschluss aufgrund übermittlungstechnischer Probleme zwischen der Übergabeschnittstelle des Verpflichteten und der berechtigten Stelle ausnahmsweise nicht möglich, so hat die Übermittlung unverzüglich nachträglich zu erfolgen. Die Überwachungskopie darf aus diesen Gründen gepuffert werden (§ 10 Satz 3 TKÜV). Die diesbezügliche Pufferung muss folgende Bedingungen erfüllen:

- Die Puffergröße muss so ausgelegt werden, dass eine Pufferzeit von 5 Minuten erfüllt wird. Dies entspricht der Ausfallzeit bis Neuetablierung der VPN-Verbindung und deckt gleichfalls Lastspitzen auf der Übertragungsstrecke ab, die im internen Netz entstehen können.
- Die Puffergröße ist so zu dimensionieren, dass das doppelte durchschnittlich am Übergabepunkt übertragene Datenvolumen gepuffert werden kann.
- Nach erneuter Herstellung der Verbindung müssen Daten aus dem Puffer nach dem FIFO-Prinzip übertragen werden. Der gesamte Datenstrom wird über einen Puffer nach dem FIFO-Prinzip übertragen. Wird die maximale Puffergröße erreicht oder kann der Puffer nicht geleert werden so sind jeweils die ältesten im Puffer vorhandenen Daten spätestens nach 5 Minuten zu verwerfen. (Somit wird erreicht, dass sollten Daten verworfen werden müssen, dies in einem zusammenhängenden Block geschieht)
- Die Pufferung muss so gestaltet werden, dass die Pufferzeit für jede zur berechtigten Stelle hergestellte TCP-Verbindung realisiert werden kann (unabhängig von der VPN-Verbindung), ohne dass sich die Puffer aller Verbindungen gegenseitig beeinflussen (z.

B. bei Überlastung eines Puffers die Mitnutzung eines anderen Puffers). Die Gestaltung eines Puffers, dessen Größe sich dynamisch anpasst und dabei das gleiche o.g. Ziel erreicht, wird ebenfalls ermöglicht, ist jedoch mit der Bundesnetzagentur abzustimmen.

3.3.2 Abstimmung der MTU-Size ~~(Auslegung der bestehenden Verpflichtung)~~

Zur Vermeidung des Fragmentierens von Datenpaketen, was zu einer erhöhten Bandbreitenbelastung führen kann, müssen die maßgeblichen Paketgrößen auf dem Weg von der Erzeugung im Erfassungspunkt des Verpflichteten bis zur Übergabe der aufbereiteten Daten an den gesicherten Übertragungsweg so bestimmt werden, dass eine Fragmentierung, insbesondere am Übergabepunkt (SINA-Box), verhindert wird.

Der Hersteller Secunet gibt für die Übertragung über die SINA-Box einen 80 Byte Overhead an, weitere 30 Byte müssen bei Nutzung von NAT-T berücksichtigt werden. Demnach muss die MTU-Size der Delivery Function auf 1380 Byte begrenzt werden. Ein Test (BNetzA, LEMF) wird dringend empfohlen, um auch mögliche Fragmentierungen im internen Netz berücksichtigen zu können.

Soweit für die Anbindung der überwachenden Netzelemente und die SINA-Box ein gemeinsames Interface benötigt wird, sind die jeweiligen Werte abzustimmen und ggf. auch mit der Bundesnetzagentur abzustimmen.

Gleiches gilt, wenn das Netzelement Jumbo-Frames unterstützt, da die hierzu verwendete MTU-Size spätestens zwischen Delivery Function und SINA-Box nicht genutzt werden kann. Zwar werden Jumbo Frames von den SINA-Boxen ab der Version 3.x unterstützt, doch entfällt diese Unterstützung derzeit durch die Verwendung des Internets als Transportnetz.

3.3.3 „alive“-Prüfung der Verfügbarkeit der Übertragungsstrecke ~~(neue Verpflichtung)~~

Zur Überwachung der Verfügbarkeit der Übertragungsstrecke zwischen Verpflichtetem und berechtigter Stelle ist eine „alive“-Prüfung nach Vorgaben des „keep-alives“ (ETSI TS 102 232-1) zu implementieren. Die „alive“-Prüfung ist für diejenigen bSn zu aktivieren, die dies bei den verpflichteten Unternehmen abfordern. Abweichend von den ETSI-Regelungen muss es möglich sein, dass durch die bS keine „Response“-Nachricht versandt wird. Dies ist notwendig, da das Versenden solcher Nachrichten durch die bS aus Sicherheitsgründen nicht immer möglich ist. Der Verpflichtete muss somit die folgenden Optionen implementieren, die für jedes Monitoring Center einer berechtigten Stelle konfigurierbar sind:

- Die „alive“-Prüfung wird auf Wunsch der berechtigten Stelle nicht genutzt.
- Die „alive“-Prüfung wird genutzt und es wird durch die bS mit einer „Response“-Nachricht geantwortet; ein Ausbleiben der „Response“-Nachricht wird durch den Verpflichteten mit einer entsprechenden Fehlermeldung quittiert.
- Die „alive“-Prüfung wird genutzt und es wird durch die bS grundsätzlich nicht mit einer „Response“-Nachricht geantwortet; Die Auswertung erfolgt durch die bS; durch den Verpflichteten wird grundsätzlich keine Fehlermeldung erzeugt. Der Verpflichtete wird in diesem Falle durch die bS über das Fehlverhalten informiert.

Die „alive“-Prüfung hat unabhängig von einer möglicherweise bestehenden Ausleitung zu erfolgen.

Die folgenden Zeiten sind zu berücksichtigen:

- Aussenden einer „alive“-Prüfung: alle 60 Minuten,
- Antwort auf eine „alive“-Prüfung per „Response“-Nachricht: innerhalb 30 Sekunden,
- Zeitraum, in dem der Verpflichtete seit Aussenden der „alive“-Prüfung eine „Response“-Nachricht erwarten kann: 60 Sekunden.

3.3.4 Standardisierte Fehlermeldungen (HI1-Messages) ~~(neue Verpflichtung)~~

Zur besseren Auswertung der Fehlermeldungen wird deren Inhalt und Format wie folgt festgelegt:

1. Bei Datenverlusten (soweit feststellbar):

   Datenverluste, die einer Maßnahme oder einer Verbindung zuzuordnen sind, müssen der berechtigten Stelle wie folgt gemeldet werden:

   - Initialmeldung mit Beginn eines Datenverlustes sowie im Folgeintervall von 5 Minuten, solange der Datenverlust in diesem Intervall anhält,
   - Nennung des Zeitpunktes des erstmaligen Datenverlustes und der Angabe des Datenverlustes (quantitativ) seit der letzten Meldung sowie die Gesamtmenge (MByte),
   - Angabe der betroffenen LIID, soweit diese Information verfügbar ist,
   - Format: *first missing data:* DDMMYYhhmmss; *data loss: Wert*; *total data loss: Wert* (Aufgrund einer existierenden Begrenzung des ETSI Parameters auf 256 Stellen nur Angaben der Werte in folgendem Format: 'DDMMYYhhmmss;*Wert*;*Wert*' , *Wert* steht hier als Platzhalter für die Angabe des Datenverlustes in Mbyte als ganze Zahl (integer)).

2. Bei fehlender Verbindung (Fehler bei „alive"-Prüfung)

   Bei ausbleibenden „Response"-Nachrichten (soweit diese Option durch die bS gewählt wurde) wird das Intervall der „alive"-Prüfung auf 1 Minute verkürzt. Somit kann ein Fortbestehen der Unterbrechung besser geprüft werden. Die Fehlermeldung erfolgt für das erst- und das letztmalige Feststellen der Unterbrechung mit Angabe:

   - des Zeitpunktes des erstmaligen Ausbleibens der „Response"-Nachricht,
   - der Anzahl der bisher nicht erhaltenen „Response"-Nachrichten,
   - optionale Angabe einer ID für die sendende DF,
   - Format: *first missing response:* DDMMYYhhmmss; *Wert* missing responses; *DF-ID Wert* (Aufgrund einer existierenden Begrenzung des ETSI Parameters auf 256 Stellen nur Angaben der Werte in folgendem Format: 'DDMMYYhhmmss;*Wert*;*Wert*' , *Wert* steht hier als Platzhalter für die Angabe der nicht erhaltenen Responses als ganze Zahl (integer) bzw. als Platzhalter für die Angabe der DF-ID).

   Nach Wiederherstellung der Verbindung wird das reguläre Intervall genutzt und der Zähler für die Fehlermeldungen zurückgesetzt.

3. Bei zu geringer Empfangskapazität auf Seiten der bSn

   Ist das Monitoring Center (MC) einer berechtigten Stelle nicht in der Lage, den Datenstrom vom Übergabepunkt des Verpflichteten in vollem Umfang entgegenzunehmen (z.B. Gegenstelle mit zu geringer Eingangskapazität um alle Daten korrekt entgegen nehmen zu können) und wird somit eine Pufferung auf Seiten des Verpflichteten veranlasst, so ist die Fehlermeldung „MC is blocking" zu versenden.

   Bei kompletter Blockierung der Gegestelle würde es zu Datenverlusten kommen, die die über eine Fehlermeldungen nach Nummer 1 berichtet werden.

Hinweis: Die Fehlermeldungen sollten durch den Systemadministrator der Auswertesysteme der bS ausgewertet werden.

4 Sonstige Anforderungen

Die TR TKÜV beinhaltet neben den technischen Anforderungen zur Gestaltung des Übergabepunktes zu den bSn weitere Vorgaben, die bei der technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen zu berücksichtigen sind.

4.1 Festlegung von Kennungen zur Umsetzung von Überwachungsmaßnahmen

Nachfolgend werden auf der Grundlage des § 11 Satz 6 TKÜV die Arten der Kennungen festgelegt, für die bei bestimmten Arten von Telekommunikationsanlagen neben den dort verwendeten Ziel- und Ursprungsadressen auf Grund der die Überwachung der Telekommunikation regelnden Gesetze zusätzliche Vorkehrungen für die technische Umsetzung von Überwachungsmaßnahmen zu treffen sind:

- **Kennungen in festnetzbezogenen TelefonieNnetzen ~~des PSTN, ISDN (circuit-switch domain)~~**

  - Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (z.B. 0700)
  - Bei emulierten Diensten die dort verwendeten Kennungen, wie z.B. SIP-URL, SIP-URI, TEL-URL, TEL-URI

- **Kennungen in Mobilfunknetzen ~~GSM, GPRS, UMTS (circuit-switch domain, packet data domain, multi-media domain)~~**

  - MSISDN
  - IMSI
  - IMEI
  - SIP-URL, SIP-URI, TEL-URL, TEL-URI

- **Kennungen für den Dienst E-Mail**

  - E-Mail-Adresse nach RFC 822 [24], RFC 2822 [25] (Ziel- und Ursprungsadresse)
  - Zugangskennung (Login-Name ohne Passwort, z.B. 'Username', 'Rufnummer', 'E-Mail-Adresse')
    des E-Mail-Postfachs

- **Kennungen ~~im Zusammenhang mit der Überwachung~~ des Internetzugangsweges**

  - Kennung des zugehörigen Telefonanschlusses
  - Fest zugeordnete IP-Adresse
  - Nutzerkennung, die dem Internetzugangsweg zugeordnet ist
  - Sonstige Bezeichnung für den Übertragungsweg, z.B. postalische Kennzeichnung (Installations-
    adresse) des kundenseitigen Anschlusses des Internetanschlusses

  Hinweis für Kabelnetze:
  Die technische Durchführung der Überwachung kann i.d.R. nur auf der Grundlage der Kabelmodemkennung (MAC-Adresse) durchgeführt werden. Die Nennung der MAC-Adresse in der Anordnung ist jedoch dann nicht nötig, wenn eine nennbare andere Kennung (z.B. Kennung des zugehörigen Telefonanschlusses, Installationsadresse) den Übertragungsweg ebenso eindeutig identifiziert. Bei einem Austausch des Kabelmodems entfällt in diesen Fällen die Ausfertigung einer neuen Anordnung.

  Für den Fall, dass in der Anordnung die Kennung des zugehörigen Telefonanschlusses benannt ist, müssen die organisatorischen Vorkehrungen so erfolgen, dass
  - ohne weitere Ausführungen zum Umfang der Überwachungsmaßnahme lediglich der Telefondienst bzw.
  - bei näherer Bezeichnung zum Umfang der Überwachungsmaßnahme (z.B. „nur Internetzugang“
    oder „Telefondienst und Internetzugang“) der genannte Umfang überwacht werden kann.

  Für den Fall, dass in der Anordnung die Kabelmodemadresse oder die Installationsadresse benannt, müssen die organisatorischen Vorkehrungen so erfolgen, dass
  - ohne weitere Ausführungen zum Umfang der Überwachungsmaßnahme der gesamte

Anschluss
mit Telefon- und Internetzugangsdienst bzw.
- bei näherer Bezeichnung zum Umfang der Überwachungsmaßnahme (z.B. „nur Internetzugang“
oder „nur Telefondienst) der genannte Umfang überwacht werden kann.

Umsetzung von Anordnungen bei Internetzugangswegen:
Aus Sicht der BNetzA und nach Auslegung der Rechtsvorschriften erfordert die Umsetzung solcher Maßnahmen i.d.R. ein zweistufiges Verfahren:
1. **Abfrage beim Anbieter** des Internetzugangsweges nach dem zuständigen Betreiber und der
zur Umsetzung nötigen Kennung,
2. **Ausstellung der Anordnung an den verpflichteten Betreiber** unter Angabe der erfragten
Kennung des Internetzugangsweges (der Betreiber muss weder Anbieter sein, noch diesbezügliche Kundendaten vorhalten).
Ist bekannt, dass es sich um einen sog. „nicht-entbündelten Anschluss“ handelt, ist der verpflichtete Betreiber sowie der DSL-Übertragungsweg eindeutig durch die Telefonnummer gekennzeichnet. In diesen Fällen kann der Schritt 1 eingespart werden.

Ist bei einem InternetZzugang über ein öffentliches WLAN keine der o.g. Kennungen verfügbar, so ist die für den Internetzugang relevante Kennung des Endgerätes (z. B. MAC-Adresse) zu verwenden. Soweit es sich bei der Nutzung öffentlicher WLANs nicht um registrierte Kunden handelt, ist bei der Ermittlung der gemäß § 110 TKG i.V.m. § 3 TKÜV für die Verpflichtung relevanten Teilnehmerzahl die Anzahl gleichzeitig an der gesamten TK-Anlage angeschlossener Endgeräte maßgeblich (wiederholtes Überschreiten).

Nicht von der Verpflichtung zur Überwachung der Telekommunikation betroffen sind Inhalte, die vom Betreiber des WLANs netzintern angeboten werden. Dies kann zum Beispiel eine Landingpage sein, die ein bestimmtes (betreiberinternes) Angebot enthält und von der aus der Nutzer dann die Möglichkeit bekommt, weitere Inhalte aus dem Internet aufzurufen. In diesem Falle wäre nur der Zugang ins Internet bzw. der Abruf begrenzter, über das Internet angebundener Dienste überwachungsfähig zu gestalten.

Sollte es die Gestaltung der technischen Einrichtungen nur zulassen, das gesamte Angebot, also interne Inhalte und den Zugang ins Internet, zu überwachen, kann dies nach Rücksprache mit der Bundesnetzagentur geduldet werden.

- **Kennungen für den Dienst VoIP und andere Multimediadienste, die auf SIP, H.323 oder H.248 in Verbindungen mit dem media stream (z.B. RTP) beruhen**

  - Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (z.B. 0700)
  - SIP-URL, SIP-URI, TEL-URL, TEL-URI
  - H.323 URL, H.323 ID
  - Zugangskennung (Login-Name ohne Passwort, z.B. 'Username', 'Rufnummer', SIP-URI)
  des VoIP-Accounts

4.2 Übermittlungsverfahren für die Anmeldung und Bestätigung von Funktionsprüfungen der Aufzeichnungs- und Auswerteeinrichtungen der bSn

Nach § 23 Abs. 1 Nr. 3 TKÜV bedarf eine Funktionsprüfung der Aufzeichnungs- und Auswerteeinrichtungen der bSn der vorherigen Anmeldung durch die bS sowie der Bestätigung durch die Bundesnetzagentur. Auf der Grundlage § 23 Abs. 1 Satz 9 TKÜV wird nachfolgend Form und Übermittlungsverfahren zur Anmeldung und Bestätigung festgelegt:

1. Die Bundesnetzagentur stellt den bSn ein elektronisch bearbeitbares Formular zur Verfügung, welches nach Prüfung und Ergänzung eines Prüfvermerkes zur Bestätigung an den Verpflichteten und die beantragende bS elektronisch versendet wird.

2. Die Übermittlung des Formulars zwischen berechtigter Stelle und Bundesnetzagentur sowie zwischen Bundesnetzagentur und Verpflichtetem findet per E-Mail statt.
3. Zur sicheren Übermittlung ist das Formular mittels PGP-Verfahren in einem sicheren Verschlüsselungsverfahren unter Nutzung einer RSA-Schlüssellänge von mindestens 1.024 Bit zu verschlüsseln.

Anlage AGrundsätzliche Festlegungen zur Übermittlung der Daten

Anlage A.1 Festlegungen zu FTAM und FTP

In dieser Anlage werden Festlegungen zu den Übertragungsmethoden FTAM und FTP getroffen.

Grundsätzlich werden die ASCII-kodierten Ereignisdatensätze nach Anlage B mittels des Übertragungsprotokolls FTAM über das X.25/X.31-Netz und die ASN.1-kodierten Ereignisdatensätze nach Anlage C und D mittels des Übertragungsprotokolls FTP über das Internet zur bS übertragen. Die Anlagen E und F enthalten Festlegungen, wonach die gesamte Übermittlungskopie per FTP übertragen wird.

Da die Übertragungsprotokolle FTAM und FTP jedoch unabhängig von der Kodierung der Ereignisdatensätze sind, ist den Verpflichteten die Auswahl des Übertragungsprotokolls freigestellt. Demnach können Ereignisdatensätze nach Anlage C und D ebenso über das X.25/X.31-Netz sowie Ereignisdatensätze nach Anlage B über das Internet übertragen werden.

Zum Schutz der zu übermittelnden Ereignisdatensätze wird bei Verwendung des X.25/X.31-Netzes das Dienstmerkmal Closed User Group (CUG) und bei Verwendung des Internet ein VPN eingesetzt.

Neben den Übermittlungsmethoden FTAM und FTP beinhalten die Anlagen C, D, F, G und H Anforderungen zu einer Übermittlung per TCP/IP. Die hierzu notwendigen nationalen Festlegungen bezüglich der zu nutzenden Portadressen sind in den jeweiligen Anlagen enthalten.

Anlage A.1.1 Dateiname

Mit den Übermittlungsmethoden FTP und FTAM werden Dateien transportiert. Die Gestaltung des Dateinamens richtet sich grundsätzlich nach der File naming method B des ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 [22]; die identische Beschreibung findet sich ebenso in der 3GPP-Spezifikation TS 33.108 [23].

Bei der Implementierung nach Anlage B kann der Dateiname ab der fünften Stelle frei definiert werden.

Dateiname nach File naming method B:

<Dateiname> nach dem Format **ABXYyymmddhhmmsseeeet**

wobei gilt:

AB :	Zwei ASCII-Zeichen als Kennung des Verpflichteten (*s. Anmerkung*)
XY :	Zwei ASCII-Zeichen für die Kennung der sendenden Mediation-Funktion (s. *Anmerkung*)
yy :	Zwei ASCII-Zeichen ["00"..."99"], Angabe für das Jahr (die letzten beiden Ziffern)
mm :	Zwei ASCII-Zeichen ["01"..."12"], Angabe für den Monat
dd :	Zwei ASCII-Zeichen ["01"..."31"], Angabe für den Tag
hh :	Zwei ASCII-Zeichen ["00"..."23"], Angabe für die Stunde
mm :	Zwei ASCII-Zeichen ["00"..."59"], Angabe für die Minute
ss :	Zwei ASCII-Zeichen ["00"..."59"], Angabe für die Sekunde
eeee :	Vier alphanumerische ASCII-Zeichen (A-Z, 0-9) zur Verhinderung ansonsten gleicher Dateinamen innerhalb einer Sekunde in einer Mediation-Funktion; nicht erlaubt sind kleine alphabetische ASCII-Zeichen (a-z)
t :	Ein ASCII-Zeichen zur Identifikation des Inhaltes (*s. Anmerkung*)

Anmerkung zu 'AB':

Die Kennungen der Verpflichteten werden von der Bundesnetzagentur verwaltet, um eine doppelte Verwendung zu vermeiden. Nach Vorlage des Konzeptes eines Verpflichteten vergibt die Bundesnetzagentur diese Kennung; gleichzeitig wird eine fünfstellige Operator-ID für den Verpflichteten festgelegt, die als Parameter in den Ereignisdaten übertragen wird (siehe Anlage X.2).

Anmerkung zu 'XY':

Grundsätzlich sieht die File naming method B vor, dass verschiedene sendende Mediation-Funktionen (z.B. zwei unterschiedliche FTP-Clients) eines Verpflichteten sich zumindest in dieser Kennung unterscheiden, auch wenn diese jeweils eine Datei mit ansonsten gleichen Dateinamen zu einer bestimmten bS senden würden.

Für **'X'** (3. Stelle des Dateinamens) muss grundsätzlich für die nach File naming method B vorgesehene Funktion der Unterscheidung mehrerer Mediation-Funktionen vorgesehen werden. Es sind hier die ASCII-Zeichen der Großbuchstaben A-Z sowie der Ziffern 0-9 erlaubt. Wenn jedoch nur eine Mediation-Funktion bei einem Verpflichteten vorgesehen ist (z.B. Betrieb eines FTP-Clients für die gesamte Telekommunikationsanlage), kann nach Absprache mit der Bundesnetzagentur für 'X' ein anderer Wert verwendet werden.

Da es jedoch nach der o.g. Festlegung möglich ist, mit den Übermittlungsprotokollen FTAM und FTP sowohl ASCII-kodierte als auch ASN.1-kodierte Dateien zu übertragen, ist es notwendig, dafür in den Dateinamen ein Unterscheidungskriterium einzuführen. Dies wird durch die Auswahl eines entsprechenden Wertes für **'Y'** (4. Stelle des Dateinamens) repräsentiert. Anhand des verwendeten Wertes für `Y` können zudem die Kodierungen nach den ETSI-Standards bzw. ETSI-Spezifikationen und 3GPP-Spezifikationen unterschieden werden.

Die nachfolgende Tabelle A.1.1-1 geht von der Nutzung von ASN.1-Modulen mit einem Object Identifier (OID) aus, die nach Anlage X.4 zu verwenden sind. Die weitere Tabelle A.1.1-2 gilt lediglich dann ergänzend, wenn ASN.1-Module ohne Object Identifier (OID) verwendet werden bzw. falls ältere Implementierungen nach den Anlagen C und D im Einsatz sind.

'Y' (4. Stelle)	**Bedeutung**
N	Kodierung entsprechend Anlage B (optional, mandatory für neue Implementierungen ab 01.01.2003 und bei Nutzung von FTP als Übertragungsprotokoll).
E	Kodierung entsprechend der Anlagen C, E, F.3, G und H (mandatory). ASN.1- bzw. TLV-kodierte Records nach ETSI-Standard bzw. ETSI-Spezifikation.
G	Kodierung nach Anlage D (mandatory) ASN.1- bzw. TLV-kodierte Records nach der 3GPP-Spezifikation TS 33.108 kodiert.
X	Kodierung nach Anlage E.5 oder F.2 (mandatory). XML-kodierter Inhalt einer überwachten E-Mail.

Tabelle A.1.1-1: Festlegungen zu 'Y' (Module mit OID)

'Y' (4. Stelle)	**Bedeutung**
E	Kodierung entsprechend Anlage C (mandatory). Einzelne Records nach ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 kodiert.
M	Kodierung entsprechend Anlage C (mandatory). Paketierte Records in einer Datei nach ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 kodiert.
G	Kodierung nach Anlage D (mandatory). Einzelne Records nach der 3GPP-Spezifikation TS 33.108 kodiert.
U	Kodierung nach Anlage D (mandatory). Paketierte Records in einer Datei nach der 3GPP-Spezifikation TS 33.108 kodiert.

Tabelle A.1.1-2: Ergänzende Festlegungen zu 'Y' (Module ohne OID)

Anmerkung zu 't':

Die ASCII-Zeichen, die als Werte für 't' (21. Stelle des Dateinamens) verwendet werden können, dienen zur Identifikation des Inhaltes der Datei. Die Datei kann Folgendes beinhalten:

- IRI: Ereignisdaten (Intercept Related Information)
- HI1: Administrierungsdaten; der Dateityp kann bei Implementierungen nach Anlage B frei gewählt werden

- CC(MO): Mobile Originated (MO) Content of Communication (CC) is included to the intercepted data
- CC(MT): Mobile Terminated (MT) Content of Communication (CC) is included to the intercepted data
- CC(MO&MT): Mobile Originated and Terminated (MO&MT) Content of Communication (CC) is included to the intercepted data
- national use: Übermittlung von Ereignisdaten und Nutzinformationen nach Anlagen E und F

Die nachfolgende Tabelle A.1.1.-3 gibt die möglichen Werte und ihre Interpretationen für 't' wieder.

't' (21. Stelle)	't' in Binärdarstellung	Datei beinhaltet Daten der Form:
1	0011 000**1**	IRI / HI1
2	0011 00**1**0	CC(MO)
4	0011 0**1**00	CC(MT)
6	0011 0**11**0	CC(MO&MT)
8	0011 **1**000	national use

Tabelle A.1.1-3: Festlegungen zu 't'

Beispiel für einen Dateinamen: VPEX06050410431200018

Dabei ist:

VP :	Kennung des Verpflichteten (von der Bundesnetzagentur vergeben)
E :	Kennung für E-Mail-Überwachung (da nur eine Mediation-Funktion (FTP-Client) verwendet wird)
X :	XML-kodierter Inhalt nach Anlagen E.5 und F.2
06 :	Jahr 2006
05 :	Monat Mai
04 :	Tag 04
10 :	Stunde 10
43 :	Minute 43
12 :	Sekunde 12
0001 :	Erweiterung 0001 zur Dateinamenunterscheidung
8 :	Übermittlung von Ereignisdaten und Nutzinformationen in einer Datei nach Anlage E oder F

Anlage A.1.2 Parameter

Bei der Übermittlung per FTAM bzw. FTP fungiert die Anlage des Verpflichteten als Sender (z.B. als FTP-Client) und die Anlage der bS als Empfänger (z.B. als FTP-Server). Die Festlegung der Parameter (z.B. username und password je FTP-Account) muss so gestaltet werden, dass diese seitens eines Verpflichteten pro Empfänger der bS im Vorfeld der Administrierung von Überwachungsmaßnahmen vorgeleistet werden können. Zudem wird dadurch die paketierte Übermittlung von mehreren Ereignisdatensätzen verschiedener Maßnahmen in einer Datei zu demselben FTP-Account möglich.

Dabei gilt grundsätzlich:

- Mehrere Ereignisdatensätze sowie ggf. Kopien der Nutzinformationen, die an einen Empfänger derselben bS zu senden sind, können als eine Datei behandelt werden; bei in ASN.1-kodierten Datensätzen erfolgt dies beispielsweise in einer 'IRISequence'.
- Im Rahmen einer Kommunikationsverbindung zwischen der TKA-V und dem Empfänger einer bS ist es möglich, jeweils eine Datei oder mehrere Dateien zu übertragen, soweit diese Dateien bei der TKA-V bereits vorliegen. Die Kommunikationsverbindung ist jedoch sofort nach Übermittlung der Dateien auszulösen, wenn zu diesem Zeitpunkt bei der TKA-V keine weiteren Datensätze vorliegen.

- Die FTP-Server der bS müssen ein Überschreiben von Dateien zulassen, damit bei Fehlern die Datei noch einmal gesendet werden kann.

Die Tabelle A.1.2-1 enthält die Festlegungen für die wichtigsten FTAM-Parameter und die Tabelle A.1.2-2 die wichtigsten FTP-Parameter.

FTAM-Parameter	Werte/Festlegungen	Bemerkungen
Document-type-name	FTAM-3	binär
Filename	Länge: 21 Stellen (bei Implementierungen nach Anlage B maximal 25 Stellen) Zeichen: Folgende ASCII-Zeichen sind erlaubt: Alphanumerische Zeichen (a-z, A-Z, 0-9), keine Umlaute	siehe Festlegungen nach Anlage A.1.1
Initiator-identity	Länge: Maximal 8 Stellen Kodierung: GraphicString Zeichen: Alphanumerische Zeichen (a-z, A-Z, 0-9); keine Umlaute	
Filestore-password	Länge: Maximal 8 Stellen Kodierung: GraphicString Zeichen: Alphanumerische Zeichen (a-z, A-Z, 0-9), keine Umlaute, Sonderzeichen '.', '%', '*', '!', '?', '@', '#'	
QoS-Klasse des Initiators	QoS-Klasse 0 ‘No Error Recovery’	Der Initiator muss die QoS-Klasse 0 verwenden, da der Response der die Recovery-Prozeduren nicht unterstützt
Create-password	wird bis auf Weiteres nicht genutzt	
Process title	1 3 9999 1 7	
Application process invocation identifier	leer	
Application entity qualifier	leer	
Application entity invocation id	leer	
Selectors (Presentation-, Session-, Transport-Selector)	FTAM	

Tabelle A.1.2-1: Wichtige Parameter für FTAM

FTP-Parameter	Werte/Festlegungen	Bemerkungen
document type	binary	binär

FTP-Parameter	Werte/Festlegungen	Bemerkungen
filename	Länge: 21 Stellen (bei Implementierungen nach Anlage B maximal 25 Stellen) Zeichen: Folgende ASCII-Zeichen sind erlaubt: Großbuchstaben und Ziffern (A-Z, 0-9), keine Umlaute	siehe Festlegungen nach Anlage A.1.1
LEA username pro FTP-Account einer bS	Länge: Maximal 8 Stellen Zeichen: Alphanumerische Zeichen (a-z, A-Z, 0-9), keine Umlaute	keine Verschlüsselung erforderlich da Nutzung eines VPN
LEA password pro FTP-Account einer bS	Länge: Maximal 8 Stellen Zeichen: Alphanumerische Zeichen (a-z, A-Z, 0-9), keine Umlaute, Sonderzeichen '.', '%', '*', '!', '?', '@', '#'	keine Verschlüsselung erforderlich da Nutzung eines VPN
Verzeichniswechsel	keine Anforderung	Ein Verzeichniswechsel durch den FTP-Client innerhalb des festgelegten Zielverzeichnisses ist nicht gefordert
port für data connection	20 (default value)	
port für control connection	21 (default value)	
mode	passive mode muss unterstützt werden	Der Extended passiv mode muss seitens der bS nicht unterstützt werden; d.h. der Verpflichtete muss den „einfachen“ active oder passive mode anbieten.

Tabelle A.1.2-2: Wichtige Parameter für FTP

Anlage A.2 Festlegungen zur Teilnahme am VPN

Zum Schutz des IP-basierten Übergabepunktes werden dedizierte Kryptoboxen auf der Basis der IPSec-Protokollfamilie eingesetzt, um die Teilnetze der bSn und der Verpflichteten zu einem Virtual Private Network (VPN) zu verbinden. Zur Verwaltung der zur Authentisierung dienenden kryptographischen Schlüssel wird eine Public-Key-Infrastruktur (PKI) eingerichtet, die von der Bundesnetzagentur als zentrale Zertifizierungs- und Registrierungsstelle betrieben wird. Darüber hinaus verwaltet die Bundesnetzagentur die möglichen Sicherheitsbeziehungen innerhalb einer Access Control List (ACL), die in einem Verzeichnisdienst bereitgestellt wird.

Die Kryptoboxen werden als dedizierte Systeme jeweils vor den zu schützenden Teilnetzen der bSn und der Verpflichteten platziert. Die Systeme garantieren Authentizität, Integrität und Vertraulichkeit.

Darüber hinausgehende Mechanismen zum Schutz des Übergabepunktes, wie z.B. gegen Denial of Service-Attacken bei den bSn, werden durch die Kryptoboxen nur bedingt erfüllt und müssen durch die Betreiber der jeweiligen Teilnetze eigenständig gelöst werden.

Die jeweiligen Kryptoboxen sind grundsätzlich Bestandteile der technischen Einrichtungen der bS bzw. des Verpflichteten; insofern fällt die Planung und der Betrieb (z.B. Betrieb eines SYSLOG-Servers) sowie die Wartung und Entstörung in die Zuständigkeit des jeweiligen Betreibers des Teilnetzes.

Die Anforderungen an die Kryptoboxen müssen ggf. künftig dem jeweiligen Stand der Technik angepasst werden, um das Schutzniveau weiterhin zu garantieren. Diesbezügliche Erweiterungen (z.B. Nutzung anderer Schlüssellängen) bzw. kurzfristig notwendige Änderungen der bestehenden Implementierung bei nachträglich entstandenen Sicherheitsmängeln sind von den Betreibern der jeweiligen Kryptoboxen in einem im Einzelfall festzulegenden Zeitraum – im Rahmen der von den Herstellern der Kryptoboxen zur Verfügung gestellten Erweiterungen bzw. Updates – nach Vorgabe durch die Bundesnetzagentur durchzuführen.

Netzarchitektur

Die Kryptoboxen der bSn und der Verpflichteten bilden ein Maschennetz, wobei stets gerichtete Sicherheitsbeziehungen (Punkt-zu-Punkt-Verbindungen) zwischen den TKA-Vn der Verpflichteten und den Teilnetzen der bSn etabliert werden. Verbindungen zwischen den Verpflichteten untereinander sind nicht möglich.

Die notwendigen kryptographischen Schlüssel zur Authentisierung der Kryptoboxen werden durch die Bundesnetzagentur erzeugt und nach erfolgter Registrierung auf der von den Betreibern der jeweiligen Teilnetze bereitgestellten SmartCard der Kryptobox gespeichert. Die Schlüssel zur Verschlüsselung der zu übertragenden Daten werden eigenständig durch die Kryptoboxen erzeugt und aktualisiert, sie stehen damit keinem Beteiligten zur Verfügung.

Nach der Inbetriebnahme der Kryptoboxen bauen diese eigenständig eine gesicherte Verbindung zum Verzeichnisdienst der Bundesnetzagentur auf, um die aktuelle ACL zu laden. Die weiteren Aktualisierungsprozesse der ACL erfolgen automatisch oder gesteuert durch die Bundesnetzagentur.

Die durch die Kryptoboxen erzeugten Logdaten (z.B. Erfolg eines ACL-Update, Störung) werden im Standardformat SYSLOG (UDP-Port 514) zur Weiterbearbeitung an den Log-Server des Verpflichteten bzw. der bS geleitet.

Gestaltung des Internetzugangs bzw. Übergabepunktes

Um die Eindeutigkeit der Adressierung der VPN-Endpunkte sowie der sendenden und empfangenden Einrichtungen der Verbindungsstrecke zur Übermittlung der Überwachungskopie bzw. der IRI herzustellen, werden öffentliche IP-Adressen eingesetzt. Werden vorhandene Internetstrukturen verwendet, muss i.d.R. ein separates Tunneling eingesetzt werden, um die Schutzanforderungen nach § 14 TKÜV zu erfüllen. Prinzipiell sind jedoch verschiedene Netzkonfigurationen möglich.

Die genannten Anforderungen sind bei der Beschreibung der Gestaltung des Internetzugangs bzw. Übergabepunktes im Rahmen des einzureichenden Konzeptes zu berücksichtigen.

Einsatzszenarien und Verfahrensablauf

Im Regelverfahren sind die Kryptoboxen fester Bestandteil der Teilnetze und u.a. über ihre IP-Konfiguration eindeutig innerhalb der ACL definiert. Nach erfolgter Registrierung und Schlüsselerzeugung wird der Verzeichnisdienst aktualisiert.

Eine Liste der für die Verwaltung der ACL notwendigen Daten sowie eine Beschreibung des Gesamtprozesses (Policy) wird für die am Verfahren Beteiligten bereitgestellt.

In einem Konzept, das von dem Beteiligten bei der Bundesnetzagentur einzureichen ist, sind alle Details (z.B. die für die Übermittlung vorgesehene IP-Adresse) zu nennen, damit die ACL entsprechend gepflegt werden kann. Dies gilt auch, wenn der Einsatz der Kryptoboxen bei Betreibern kleiner Telekommunikationsanlagen im Rahmen von sog. Pool-Lösungen auf Grund von § 21 TKÜV vorgesehen ist.

Sonstige Regelungen und Hinweise

Neben diesen Regelungen zur Teilnahme am VPN gelten die nachfolgenden normativen Einzelregelungen bzw. Hinweise:

- Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy).
  Die Anlage X.3 gibt den Stand bei Herausgabe dieser Ausgabe der TR TKÜV wieder.
- Übersicht „Beschreibung Gesamtprozess Teilnahme am VPN-Verfahren“.
- Antrag zur Teilnahme am VPN für die Verpflichteten sowie für die bSn (Registrierung und technische Beschreibung der Infrastruktur des Teilnetzes mit IP-Adressen und Optionsauswahl).

Die Dokumente werden bereitgestellt auf der Internetseite der Bundesnetzagentur unter: http://www.bundesnetzagentur.de/tku

Übersicht zu den einsetzbaren Kryptoboxen

Diejenigen Kryptoboxen, die die systemtechnischen Basisanforderungen sowie die Anforderungen zur Interoperabilität erfüllen, werden in der folgenden Tabelle gelistet.

Nr.	Hersteller	Produktname	Ansprechpartner
1	**secunet Security Networks AG** Ammonstraße 74 01067 Dresden www.secunet.com	SINA-Box	Division Public Authorities E-Mail: Info@secunet.com Tel: 0201/5454-0

Anlage A.3 Übermittlung von HI1- und zusätzlichen Ereignissen

Die dieser TR TKÜV zugrunde liegenden internationalen Standards und Spezifikationen beschreiben grundsätzlich die Übermittlung und den Inhalt der zu übermittelnden Ereignisdatensätze.

Dazu gehört auch die Übermittlung von sog. HI1-Ereignisdaten, die bei Aktivierung, Deaktivierung oder Modifizierung von Überwachungsmaßnahmen sowie bei Alarmmeldungen an die bS zu übermitteln sind. Hierzu steht grundsätzlich das bei ETSI spezifizierte ASN1-Modul 'HI1NotificationOperations' (ETSI TS 101 671, Annex D.4, ab Version 3) oder das national spezifizierte ASN.1-Modul nach Anlage A.3.2 zur Verfügung. Zur Übermittlung der tatsächlich betroffenen Kennung bei der Aktivierung einer Überwachungsmaßnahme nach § 5 Abs. 5 TKÜV ist das ASN.1-Modul 'HI1NotificationOperations' ab Version 6 um einen entsprechenden Parameter erweitert worden.

Darüber hinaus muss auch das nationale ASN.1-Modul zur Übermittlung folgender Ereignisse genutzt werden, da hierfür in den internationalen Spezifikationen und Standards keine Parameter definiert sind:

- Herstellereigene Dienste und Dienstmerkmale (sofern diese nicht von den HI2-Modulen der Standards bzw. Spezifikationen abgedeckt werden),
- Ereignisse zur Aktivierung, Deaktivierung oder Modifikation von Diensten und Dienstmerkmalen (z.B. Erstellen einer Verteilerliste in einer UMS per Webzugang),
- Ereignisse zu Einstellungen bezüglich der Überwachung des Dienstes E-Mail bei Verwendung des ETSI TS 102 232-02 (siehe Anlage F.3).

Das ASN1-Modul 'HI1NotificationOperations' und das nationale ASN.1-Modul werden je nach verwendetem Standard bzw. Spezifikation unterschiedlich integriert.

Anlage A.3.1 Möglichkeiten der Übermittlung

Die folgende Tabelle erläutert die grundsätzlichen Möglichkeiten der Integration des ASN1-Moduls 'HI1NotificationOperations' sowie des nationalen ASN.1-Moduls:

Standard bzw. Spezifikation	**Methode**	**Erläuterung**
ES 201 671 / TS 101 671 [1)]	Übermittlung des ASN.1-Moduls '**HI1NotificationOperations**' mit dem integrierten Parameter 'National-HI1-ASN1parameters'	Durch das ASN.1-Modul können die o.g. HI1-Ereignisse direkt zur bS übermittelt werden; zudem enthält es den Parameter 'National-HI1-ASN1parameters', mit dem auch die o.g. zusätzlichen Ereignisse übermittelt werden können. Die notwendigen Festlegungen enthält Anlage A.3.2.1.
	Übermittlung des ASN.1-Parameters 'National-HI2-ASN1parameters' durch das HI2-Modul '**HI2Operations**'	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisse sowie die zusätzlichen Ereignisse im HI2-Modul integrieren. Die notwendigen Festlegungen enthält Anlage A.3.2.2.
3GPP TS 33.108 [1)]	Übermittlung des ASN.1-Parameters 'National-HI2-ASN1parameters' durch das HI2-Modul 'HI2Operations', welches wiederum in die Module **'UmtsHI2Operations'** und **'UmtsCS-HI2Operations'** importiert wird.	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisse sowie die zusätzlichen Ereignisse im HI2-Modul integrieren. Vor der Übermittlung wird dieses HI2-Modul in das jeweilige UMTS-Modul importiert. Die notwendigen Festlegungen enthält Anlage A.3.2.2.

	Übermittlung des ASN.1-Parameters 'National-HI3-ASN1parameters' durch das HI2-Modul '**Umts-HI3-PS**'	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisse sowie die zusätzlichen Ereignisse im HI2-Modul integrieren. Die notwendigen Festlegungen enthält Anlage A.3.2.3.
TS 102 232-01	Import des gesamten ASN.1-Moduls '**HI1NotificationOperations**' durch das Modul '**LI-PS-PDU**'	Durch den Import des gesamten Moduls können die o.g. HI1-Ereignisse direkt zur bS übermittelt werden; zudem enthält das HI1-Modul den Parameter 'National-HI1-ASN1parameter', mit dem auch die o.g. zusätzlichen Ereignisse übermittelt werden können. Die notwendigen Festlegungen zum HI1-Modul enthält Anlage A.3.2.1

Tabelle A.3-1 Übermittlung der HI1- und zusätzlicher Ereignisse

[1)] Nach ES 201 671/TS 101671 bzw. 3GPP TS 33.108 besteht grundsätzlich auch die Möglichkeit, die Ereignisse mittels des ASN.-1 Parameters '**National-Parameters**' über das HI2-Modul 'HI2Operations' zu übermitteln. Der ASN.1-Parameter definiert einen Octettstring, in dem die HI1-Ereignisse und die zusätzlichen Ereignisse erst indirekt durch ein weiteres ASN.1-Modul eingebunden werden. Da diese Methode seitens der Programmierung und der Auswertung sehr aufwendig ist, kann diese Methode bei neuen Implementierungen nicht mehr verwendet werden (siehe Anlage A3.2.4).

Anlage A.3.2 Das nationale ASN.1-Modul 'Natparas'

Diese Anlage enthält die ASN.1-Beschreibung des nationalen Moduls '**Natparas**' zur Übermittlung der HI1-Ereignisse sowie der zusätzlichen Ereignisse nach Tabelle A.3-1. Wird das Modul im HI1-Modul 'HI1NotificationOperations' eingesetzt, müssen die Parameter für die HI1-Ereignisse nur einmal übermittelt werden.

Da diese ASN.1-Beschreibung relativ oft durch neu hinzukommende Parameter ergänzt werden muss, gibt diese Anlage nur den Stand bei der Herausgabe der entsprechenden Version der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Parameter mit den Betroffenen ab und ergänzt das ASN.1-Modul. Die jeweils aktuelle Version der ASN.1-Beschreibung der nationalen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur zum Download bereitgestellt:

http://www.bundesnetzagentur.de/tku

ASN.1-Modul 'Natparas', Version 8

```
-- Nationale Parameter (Content defined by national law)
-- Version dieser ASN.1-Spezifikation der nationalen Parameter: '8',
-- einzufügen in den Parameter "specificationVersion"
-- Neuere Versionen sind abwärtskompatibel.

NatParameter
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

Natparas ::= SEQUENCE {

application  [0] ENUMERATED
  {hI2-201671 (1),
        -- Bei Nutzung der HI2/3-Module von ES 201 671 oder TS 101 671
   hI2-33108 (2),
        -- Bei Nutzung der HI2/3-Module von 3GPP TS 33 108
   hI2-101233 (3),
        -- Bei Nutzung der HI2/3-Module von TS 102 233 bzw. TS 102 232-2
   hI2-101234 (4),
        -- Bei Nutzung der HI2/3-Module von TS 102 234 bzw. TS 102 232-3
   ...,
   hi2-102232 (5),
        -- Bei Nutzung der Nutzung der Übermittlungsmethode nach TS 102 232 bzw. TS 102 232-1
        -- Diese Nutzung beinhaltet Tag 3 und 4 sowie alle weiteren HI2/3-Module, die
        -- mittels TS 102 232 bzw. TS 102 232-1 übermittelt werden
   hi1-201671 (6)
        -- Bei Nutzung des Moduls HI1-Moduls von ES 201 671 oder TS 101 671
  } OPTIONAL,
        -- Dieser Parameter wurde erst in version 3 aufgenommen
```

```
        -- Für Implementationen auf Basis der Versionen 1 und 2 ist der Parameter optional,
        -- für Implementationen ab version 3 ist dieser Parameter mandatory

natVersion  [1] SEQUENCE {
    country  [0] OCTET STRING (SIZE (1..4)),
         -- coded in the same format as country codes [EN 300 356-1 to 20]
         -- e.g. 49 for Germany
    specificationVersion [1] INTEGER (0..255)
    },

notification  [2] SEQUENCE {
    liOperation-type [1] ENUMERATED {
      liActivated (1),
      liDeactivated (2),
      liModified (3)
      } OPTIONAL,
         -- Nicht erforderlich in Verbindung mit dem HI1-Modul aus TS 101 671,
         -- da dort ein operation-type vorgesehen ist
    alarms-indicator  [2] Alarm-Indicator OPTIONAL,
         -- Werte für Alarm-Indicator, alle Zeichen im ASCII-Format
         -- Nicht erforderlich in Verbindung mit dem HI1-Modul aus TS 101 671,
         -- da dort ein alarm-indicator vorgsehen ist
    li-end   [3] TimeStamp OPTIONAL,
         -- 'time of expiry of the monitoring order'(liActivated-, liModified-
         -- Records)
    target   [4] OCTET STRING (SIZE (1..256)) OPTIONAL
         -- im Format: freier ASCII-kodierter Text
         -- tatsächlich überwachte Kennung nach § 5 Abs. 5 TKÜV
         -- Aus Gründen der Rückwärtskompatibilität als optional
  } OPTIONAL,

sCIGerman  [3] SEQUENCE {
    typeOfData [0] SciType   OPTIONAL,
    sciResult [1] SciResultMode OPTIONAL,
    sciData  [2] OCTET STRING (SIZE (1..256)) OPTIONAL
    } OPTIONAL,

common    [4] CommonMode OPTIONAL,

-- moduls of the manufactures
          alcatel  [5] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          ericsson  [6] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          lucent   [7] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          nortel   [8] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          siemens  [9] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          gten    [10] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification

          md-usag-nokia  [20] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          md-usag-comverse [21] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          md-usag-motorola [22] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          md-usag-siemens [23] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          md-usag-unisys  [24] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          md-usag-ericsson [25] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          md-usag-nortel  [26] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
          ...,

e-mail-type  [100] ENUMERATED
     -- Bei Implementierungen auf der Grundlage ab Ausgabe 5.1 der TR TKUE
     -- muss dieser Parameter nicht besetzt werden
   {
    iMAP (1),
    webmail(2),
    ...,
    lMTP (3),
    iMAPS (4),
```

```
    sSMTP (5),
    pOP3S (6)
  } OPTIONAL,


e-mail-add   [101] SEQUENCE
  {
   event [1] Event,
   explain[2] Explain,
   ...
  } OPTIONAL
}

-- *************************** Parameter begin **********************
Event   ::= ENUMERATED
 {
  grouplist-create (0),
  grouplist-change (1),
  grouplist-delete (2),
  -- Einstellungen zu Versandlisten

  messaging-create (3),
  messaging-active  (4),
  messaging-change (5),
  messaging-delete (6),
  -- Einstellungen zum Messaging-Dienst

  forwarding-create (7),
  forwarding-active (8),
  forwarding-change (9),
  forwarding-delete (10),
  -- Einstellungen zum Weiterleitungs-Dienst

  email-new  (11),
  email-change (12),
  email-delete  (13),
  -- Einstellung zu E-Mail-Addressen

  sonstiges (14),
  -- Dieser Parameter muss genutzt werden, wenn zu den genannten Kategorien ein
  -- weiterer, unterschiedlicher Parameter erforderlich ist
  ...

  -- Wird beim Messaging- oder Weiterleitungs-Dienst ein neue Einstellung damit auch
  -- aktiv, muss nur das activ-event berichtet werden;
 }

Explain  ::= OCTET STRING (SIZE (1..256))
  -- Angabe der durchgeführten Einstellungen (Parameter)
  -- im Format: freier ASCII-kodierter Text

Alarm-Indicator  ::= OCTET STRING    (SIZE (1 .. 25))
  --Provides information about alarms (free format)
        -- CC-F:ccc = CC-Link Failure, ccc ist der Cause Value der Release Messag
        -- als Dezimalwert
        -- MD-OFF:DDMMYYhhmm = Datum und Uhrzeit des Ausfalls oder Abschaltens des
        -- Mediation Devices (optional)
        -- MD-ON:DDMMYYhhmm = Datum und Uhrzeit der (Wieder)Inbetriebnahme des
        -- Mediation Devices (optional)
        -- LEMF-IRI-OFF:DDMMYYhhmm = Datum und Uhrzeit des Beginns der Nichterreichbarkeit
        -- des LEMF für IRI (optional)
        -- LEMF-IRI-ON:DDMMYYhhmm = Datum und Uhrzeit der (Wieder)Erreichbarkeit des
        -- LEMF für IRI (optional)

CommonMode  ::= SEQUENCE {
  inControlled [0] InControlMode OPTIONAL,
  -- spvInfo [1] SpvInfoMode OPTIONAL
  ...
  }

InControlMode  ::= SEQUENCE {
  correlationNumber [0] INTEGER (0..65535) OPTIONAL,
  dataContent  [1] OCTET STRING (SIZE (1 .. 100))
      }

SciType  ::= ENUMERATED {
  undefined (0),
  analogSubscriber (1),
```

```
  dss1FunctionalProt (2),
  dss1KeypadProt (3),
  einsTr6FunctionalProt (4),
  mobileNetProt (5),
  systemSpecific (6)
  }


SciResultMode  ::= ENUMERATED {
  undefined (0),
  successful (1),
  unsuccessful (2),
  rejected (3),
  intermediateInfo (4)
       }

TimeStamp   ::= CHOICE
         {
             localTime [0] LocalTimeStamp,
             utcTime   [1] UTCTime
         -- TimeStamp wie in ETSI ETS 201 671
         }

LocalTimeStamp ::= SEQUENCE
         {
              generalizedTime   [0] GeneralizedTime,
              winterSummerIndication  [1] ENUMERATED {
                          notProvided(0),
                          winterTime(1),
                          summerTime(2),
                          ...
                          }
}
END -- Natparas
```

Anlage A.3.2.1 Übermittlung mit dem ASN.1-Modul 'HI1NotificationOperations'

Diese Anlage enthält die Methode zur Übermittlung der HI1- und zusätzlicher Ereignisse mittels des ASN.1-Moduls 'HI1NotificationOperations' ab der Version 3. Frühere Versionen des Moduls sind nicht zugelassen, da diese noch keinen OID enthalten.

Die gleiche Beschreibung wird verwendet, wenn das gesamte Modul 'HI1NotificationOperations' in das Modul **'LI-PS-PDU'** gemäß Anlage G für den Internetzugangsweg importiert wird.

```
HI1NotificationOperations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi1(0)
 notificationOperations(1) version5(5)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
 OPERATION,
 ERROR
  FROM Remote-Operations-Information-Objects
  {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

 CommunicationIdentifier,
 TimeStamp,
 LawfulInterceptionIdentifier
  FROM HI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
              hi2(1) version8(8)}

 Natparas
  FROM NatParameter

 Natparas2
  FROM NatParameter2;


National-HI1-ASN1parameters  ::= SEQUENCE
```

```
{
 domainID  [0] OBJECT IDENTIFIER (hi1OperationId) OPTIONAL,
  -- Once using FTP delivery mechanism.
 countryCode  [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [67],
  -- the country to which the parameters inserted after the extension marker apply.
 ...,
       -- In case a given country wants to use additional national parameters according to
       -- its law, these national parameters should be defined using the ASN.1 syntax and
       -- added after the extension marker (...).
       -- It is recommended that "version parameter" and "vendor identification parameter"
       —- are included in the national parameters definition. Vendor identifications can be
       -- retrieved from IANA web site (see annex H). Besides, it is recommended to avoid
       -- using tags from 240 to 255 in a formal type definition.

 natparas  [2] Natparas,
  -- Import von TR TKÜV, Teil A, Anlage A.3.2

 natparas2 [3] Natparas2
  -- Import von TR TKÜV, Teil C, Abschnitt 3.2
}

END -- HI1NotificationOperations
```

Anlage A.3.2.2 Implementierung im ASN.1-Modul 'HI2Operations'

Diese Anlage enthält die Implementierung im ASN.1-Modul 'HI2Operations'. Die gleiche Beschreibung wird verwendet, wenn das gesamte Modul 'HI2Operations' in die Module **'UmtsHI2Operations'** und **'UmtsCS-HI2Operations'** gemäß Anlage D importiert wird.

```
HI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
 version8(8)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS OPERATION,
 ERROR
  FROM Remote-Operations-Information-Objects
  {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

 UmtsQos,
 IMSevent
  FROM UmtsHI2Operations
              {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
               threeGPP(4) hi2(1) r6(6) version-5(5)}

 Natparas
  FROM NatParameter

 Natparas2
  FROM NatParameter2;
```

```
IRI-Parameters ::= SEQUENCE
{
  domainID   [0] OBJECT IDENTIFIER (hi2OperationId) OPTIONAL,
  -- for the sending entity the inclusion of the Object Identifier is mandatory
  national-HI2-ASN1parameters [255] National-HI2-ASN1parameters OPTIONAL
}
```

```
National-HI2-ASN1parameters ::= SEQUENCE
{
 countryCode  [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [67],
  -- the country to which the parameters inserted after the extension marker apply.
 ...
       -- In case a given country wants to use additional national parameters according to
       -- its law, these national parameters should be defined using the ASN.1 syntax and
       -- added after the extension marker (...).
       -- It is recommended that "version parameter" and "vendor identification parameter"
       -- are included in the national parameters definition. Vendor identifications can be
       -- retrieved from the IANA web site (see annex H). Besides, it is recommended to
       -- avoid using tags from 240 to 255 in a formal type definition.

 natparas  [2] Natparas,
  -- Import von TR TKÜV, Teil A, Anlage A.3.2

 natparas2 [3] Natparas2
  -- Import von TR TKÜV, Teil C, Abschnitt 3.2
}

END -- HI2Operations
```

Anlage A.3.2.3 Implementierung im ASN.1-Modul 'Umts-HI3-PS'

Diese Anlage enthält die Implementierung im ASN.1-Modul 'Umts-HI3-PS':

```
Umts-HI3-PS
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
 hi3(2) r6(6) version-3(3)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
 GPRSCorrelationNumber
 FROM UmtsHI2Operations
 {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
        threeGPP(4)  hi2(1) r6(6) version-6(6)}

 LawfulInterceptionIdentifier,
 TimeStamp
 FROM HI2Operations
 {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
 version7(7)}

 Natparas
  FROM NatParameter

 Natparas2
  FROM NatParameter2;


National-HI3-ASN1parameters ::= SEQUENCE
{
 countryCode  [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [39],
  -- the country to which the parameters inserted after the extension marker apply
 ...,
       -- In case a given country wants to use additional national parameters according to its
 -- law, these national parameters should be defined using the ASN.1 syntax and added after
 -- the extension marker (...).
 -- It is recommended that "version parameter" and "vendor identification parameter" are
 -- included in the national parameters definition. Vendor identifications can be
 -- retrieved from IANA web site. It is recommended to avoid
 -- using tags from 240 to 255 in a formal type definition.

 natparas  [2] Natparas,
  -- Import von TR TKÜV, Teil A, Anlage A.3.2

 natparas2 [3] Natparas2
  -- Import von TR TKÜV, Teil C, Abschnitt 3.2
}

END-- OF Umts-HI3-PS
```

Anlage A.3.2.4 Übermittlung mit dem ASN.1-Parameter 'National-Parameters'

Diese Anlage enthält die Methode zur Übermittlung der HI1- und zusätzlicher Ereignisse mittels des ASN.1-Parameters 'National-Parameters' im Modul HI2Operations der ES 201 671/TS 101 671 bis zur Version 4 bzw. im Modul UmtsHI2Operations' bis zur Version 6.6.0.

Der ASN.1-Parameter definiert einen Octettstring, in dem die HI1-Ereignisse und die zusätzlichen Ereignisse erst indirekt durch ein weiteres ASN.1-Modul eingebunden werden. Da diese Methode seitens der Programmierung und der Auswertung sehr aufwendig ist, wurde sie in den Standards bzw. Spezifikationen durch die Methode gemäß Anlage A.3.2.3 ersetzt und steht daher für neue Implementierungen nicht mehr zur Verfügung.

Erläuterung anhand eines konkreten Beispiels:

Die nach den Basic Encoding Rules (BER) kodierten Daten sind nach dem Kodierprozess in den mittels ASN.1-Typ

'National-Parameters ::= SET SIZE (1..40) OF OCTET STRING (SIZE (1..256))'

bereitgestellten Container von maximal 40 x 256 Oktetts einzufügen (siehe auch nachfolgende Skizze).

Ein Beispiel mit SIZE (3):

T	**L**	**V (siehe grüner Bereich)**		
SET = 'B0	xx			
		T	**L**	**V (siehe roter Bereich)**
		OCTETSTRING = '04	Y1	ASN.1-kodierte nationale Parameter, beginnend mit 'Natparas ::= SEQUENCE { ', wobei die einzelnen Oktetts fortlaufend eingetragen werden: T('30)LV1 TLV2 TLV3 ... TLVm (auch nested)
		'04	Y2	TLVm+1 TLVm+2 TLVm+3...TLVn
		'04	Y3	TLVn+1 TLVn+2 TLVn+3...TLVo

Kodierung SET (SIZE (3) OF
Kodierung OCTET STRING
Kodierung der nationalen Parameter, beginnend mit SEQUENCE = '30

Konkretes Beispiel: Report-Record bei Aktivierung einer Überwachungsmaßnahme:

Dieses Beispiel zeigt den Inhalt des nationalen Parameters für das Ereignis 'Aktivierung einer Überwachungsmaßnahme - liActivated' sowie die Einbettung in einen Report-Record.

Die nächste Zeile enthält den kompletten OCTET STRING des nationalen Parameters, der dem roten Bereich der obigen Skizze entspricht: **30 0E A1 07 80 02 34 39 81 01 01 A2 03 81 01 01**

Nachfolgend sind die einzelnen Bytes erläutert:

30 0E sequence, length 14 (universal type, constructed)
A1 07 natVersion (context specific type, constructed)
80 02 34 39 country code (context specific type primitiv, gefüllt mit ASCII-Zeichen '49')
81 01 01 versions-number (context specific type, primitiv, integer '1')
A2 03 notification (context specific type, constructed)
81 01 01 liOperation-type (context specific type, primitiv, liActivated)

Die nächsten Zeilen enthalten den kompletten Report-Record einschließlich des nationalen Parameters:

```
A4 44 97 01 02 81 09 42 4B 41 2D 31 32 33 34 35 A2 09 A1 07 80 05 34 39 31 32 33 A3 15
A0 13 80 0E 32 30 30 32 30 38 30 39 31 35 33 35 31 32 81 01 00 B0 12 04 10 30 0E A1 07
80 02 34 39 81 01 01 A2 03 81 01 01
```

Anlage A.4 Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Ist die Übermittlung der Überwachungskopie zur bS nicht möglich (z.B. durch eine Störung in der Sendeeinrichtung der TKA-V, Überlast im Transitnetz oder wenn die Anschlüsse der bS besetzt sind) gilt grundsätzlich die Vorgabe des § 10 TKÜV, wonach die Ereignisdatensätze unverzüglich nachträglich übermittelt werden müssen.

Eine Verhinderung oder Verzögerung der zu überwachenden Telekommunikation oder eine Speicherung des Inhalts der Überwachungskopie aus diesen Gründen ist nicht zulässig. Telekommunikationsinhalte dürfen lediglich gepuffert werden, sofern dies für den ungestörten Funktionsablauf aus technischen, insbesondere übermittlungstechnischen Gründen erforderlich ist.

Bei nachfolgenden zu überwachenden Telekommunikationsereignissen sind die Verbindungsversuche für die Übermittlung der Überwachungskopie erneut zu initiieren, soweit im Einzelfall keine abweichenden Vereinbarungen mit der berechtigten Stelle getroffen wurden (z.B. bei andauernder Störung).

Technische Umsetzung

Erste wiederholte Verbindungsaufbauversuche

Tritt ein Hindernis bei der Übermittlung der Überwachungskopie auf, sind zunächst drei weitere Verbindungsaufbauversuche zu unternehmen. Bei Nutzung von leitungsvermittelten Verbindungen erfolgen diese im Abstand von je 5 bis 10 Sekunden, bei Nutzung von FTAM, FTP oder TCP/IP im Abstand von bis zu wenigen Minuten. Kann die Verbindung zur bS nach diesen drei Versuchen wieder hergestellt werden, sind die Ereignisdaten sowie die Kopie des Telekommunikationsinhaltes ab dem Wiederherstellungszeitpunkt zu übermitteln.

Kann die Überwachungskopie nach diesen wiederholten Verbindungsaufbauversuchen nicht zur bS übermittelt werden, müssen die Ereignisdatensätze zur nachträglichen Übermittlung gespeichert werden.

Weitere Verbindungsaufbauversuche

Nach den drei wiederholten Verbindungsaufbauversuchen sind diese für einen Zeitraum von 24 Stunden in angemessenen Zeitintervallen so lange zu wiederholen, bis sie erfolgreich sind.

Ist in diesem erweiterten Zeitraum eine Übermittlung nicht möglich, sind die Ereignisdaten auszudrucken oder auf einem Speichermedium (z. B. CD) zu speichern, in geeigneter Weise an die bS zu übermitteln (z. B. gesicherte E-Mail) und in der TKA-V zu löschen. Die vorgenannte 24-Stunden-Frist kann der Verpflichtete auf 1 Woche ausdehnen, sofern sichergestellt ist, dass der bS die Ereignisdaten zu bestimmten Maßnahmen auf deren Anforderung früher bereitgestellt werden können (z. B. auf dem für den Fehlerfall vorgesehenen Ersatzweg).

Kann in diesem erweiterten Zeitraum die Verbindung zur bS wieder aufgebaut werden, ist neben den Ereignisdaten auch die Kopie des Telekommunikationsinhaltes ab dem Wiederherstellungszeitpunkt zu übermitteln.

Bei leitungsvermittelnden Fest- und Mobilfunknetzen müssen nach den o.g. drei weiteren Verbindungsversuchen jedoch keine erneuten Verbindungsversuche mehr für die Übermittlung der Kopie des Telekommunikationsinhaltes zur bS unternommen werden, soweit der Übergabepunkt nach Anlagen B bzw. C gestaltet wurde.

Erkannte Stör- und Fehlerfälle, die dazu führen, dass die Überwachung der Telekommunikation oder die Übermittlung der Überwachungskopie beeinträchtig ist, sind als Alarmmeldungen unverzüglich in einem gesonderten Ereignisdatensatz oder auf andere Weise an die bS zu senden bzw. zu melden. Wenn die Übermittlung der Ereignisdatensätze von einer Störung selbst betroffen ist, müssen diese Alarme dennoch generiert werden, um sie zur Dokumentation der Störung nach Wiederherstellung der Übermittlungsfunktion zu versenden oder per Speichermedium zu übermitteln. In Mobilfunknetzen sind die Angaben

über Störungen, die sich nur in regional begrenzten Bereichen des Netzes auswirken, nur auf Nachfrage der bSn in dann geeigneter Weise (z.B. per Fax oder E-Mail) zu machen

Anlage BÜbergabepunkt für leitungsvermittelnde Netze (national)

Hinweis zur Nutzung bestehender Anlagen basierend auf Ausleitungen per ISDN oder X.25/X.31:

Aufgrund des mittelfristig absehbaren Abschaltens ISDN-basierter Technik muss auch die entsprechende Ausleitung, basierend auf dieser Technik, mittelfristig angepasst werden. Grundsätzlich sind neue Implementierungen, deren Ausleitung auf ISDN basiert, nicht mehr möglich. Bestehende Anlagen sind bis spätestens zum 31.12.2021 auf Ausleitungen nach Anlage D bzw. Anlage H umzustellen. Ist die Versorgung über den bestehenden Anbieter innerhalb dieser Frist nicht mehr möglich, so kann auch ein Wechsel zu einem alternativen Anbieter, der weiterhin ISDN anbietet, erfolgen. Zudem ist eine Vereinheitlichung der Schnittstellen vorgesehen: Aus diesem Grund sind bis zum 31.12.2017 alle Ausleitungen über X.25/X.31 durch Ausleitungen per FTP zu ersetzen.

Diese Anlage beschreibt den national festgelegten Übergabepunkt für leitungsvermittelnde Netze (ISDN, PSTN, GSM) und erfolgte vor der Aufnahme des ETSI-Standards ES 201 671 bzw. den ETSI-Spezifikationen TS 101 671 (siehe Anlage C) sowie TS 101 232-06 (siehe Anlage H) in die TR TKÜV.

Seit dem 01.01.2005 kann der Übergabepunkt für leitungsvermittelnde Netze nach dieser Anlage nur noch für Erweiterungen solcher Netze verwendet werden.

Für neue leitungsvermittelnde Netze gelten die Beschreibungen nach Anlage C sowie Anlage H.

Neben den Anforderungen nach Teil A, Abschnitte 3 und 4, sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Kopie der Nutzinformation erfolgt per ISDN-Doppelstiche und ist in dieser Anlage B beschrieben. Die Übermittlung der Ereignisdaten (ASCII-Dateien) kann wahlweise per FTAM/X.25 oder FTP/Internet erfolgen. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten
Anlage A.2	Teilnahme am VPN mittels Kryptobox Wird die Übermittlung der Ereignisdaten per FTP/Internet vorgenommen werden, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage B.1 Allgemeine Anforderungen

Die nachfolgenden Anforderungen ergänzen die in Abschnitt 3.1 gemachten Aussagen zur Gestaltung des Übergabepunktes auf der Grundlage von nationalen Festlegungen.

Anlage B.1.1 Referenznummer und Zuordnungsnummer

Bei der Übermittlung zur bS ist die Kopie der Nutzinformation und der zugehörigen Ereignisdatensatz so zu kennzeichnen, dass sie einander eindeutig zugeordnet werden können.

Hierzu erhält jede Überwachungsmaßnahme eine Referenznummer, die mit den Ereignisdaten in den Datensätzen der jeweiligen Überwachungsmaßnahme zur bS zu übermitteln ist (siehe Anlage B.2.4). Zusätzlich müssen die einzelnen Verbindungen innerhalb einer Überwachungsmaßnahme mit einer für die jeweilige Verbindung eindeutigen Zuordnungsnummer versehen werden (siehe Anlage B.2.5). Die Zuordnungsnummer hat Werte zwischen 1 und 65535. Sie wird sowohl für die zu der bS aufzubauenden Verbindungen zur Übermittlung der Kopie der Nutzinformation als auch bei allen zugehörigen Ereignisdatensätzen verwendet. Bei den Verbindungen von der TKA-V zur bS zur Übermittlung der Kopie der Nutzinformationen wird die Zuordnungsnummer in der Subadresse des Gerufenen (hier: der bS) übermittelt. Hierzu werden zwei Oktetts (Bytes) der im Dienstmerkmal ‘Subadresse’ zur Verfügung stehenden 20 Oktetts verwendet (Oktetts 4 und 5), wobei Oktett 5 das höherwertige Byte des Zählers ist (siehe auch Anlage B.3.1).

Bei den zugehörigen Ereignisdatensätzen ist die Zuordnungsnummer der zu überwachenden Verbindung in das hierfür vorgesehene Feld einzusetzen (siehe Anlage B.2.5).

Zusätzlich kann die TKA-V ein weiteres Kriterium einfügen, z. B. in Mobilfunknetzen die Kennung des MSC. Wird eine solche Zusatzkennung benutzt, ist sie bei den Verbindungen zur Übermittlung der Kopie der Nutzinformationen in den Oktetts 7 und 8 der Subadresse des gerufenen Teilnehmers (hier: der bS) zu übermitteln (siehe Anlage B.3.1), im zugehörigen Datensatz mit den Ereignisdaten zusätzlich zur Zuordnungsnummer.

Anlage B.1.2 Übermittlung der Kopie der Nutzinformationen

Zur Übermittlung der Kopie der Nutzinformation werden von der TKA-V zwei transparente (siehe hierzu unten: Anmerkung 1) Wählverbindungen (Circuit-mode 64 kbit/s unrestricted, ETS 300 108) zur bS aufgebaut, von denen eine die Kopie der vom züA gesendeten Nutzinformationen und die andere die Kopie der für den züA bestimmten Nutzinformationen zu den technischen Einrichtungen der bS überträgt (siehe hierzu unten: Anmerkung 2).

Der bS muss mitgeteilt werden, welche der beiden Verbindungen die Sende- bzw. Empfangsseite des züA ist. Hierzu werden die Bits 1 und 2 im Oktett 6 der Subadresse der Called Party verwendet (siehe Anlage B.3.1).

Anmerkung 1: Transparente Verbindung bedeutet, dass

a) bei teilnehmergleicher Anschaltung der TKA-V an das Transitnetz (z. B. ISDN-Basis- oder -Primärmultiplexanschluss mit DSS1-Signalisierung) der Dienst ‘Circuit-mode 64 kbit/s unrestricted 8 kHz structured bearer service category (ETS 300 108)’ und

b) bei netzgleicher Anschaltung der TKA-V an das Transitnetz (Schnittstelle nach ITU-T-Empfehlung G.703 mit ZGS-Nr.7-Signalisierung) das entsprechende Übertragungsmedium (64 kbit/s unrestricted) anzufordern ist.

Anmerkung 2: Bei der Beteiligung mehrerer Teilnehmer an einem Gespräch (Konferenzgespräch) enthalten die für den züA bestimmten Nutzinformationen die gesendeten Nutzinformationen aller anderen Teilnehmer (Summensignal). Somit wird über die eine Verbindung zur bS die Kopie dieses Summensignals übertragen. Die Kopie der vom züA ausgehenden Telekommunikation (Einzelsignal des züA) ist über die zweite Verbindung zur bS zu übertragen (Richtungstrennung).

Weiterhin ist bereits beim Aufbau der Verbindungen zur bS zu signalisieren, ob die Nutzinformation ‘Sprache’ oder ‘Audio-Information’ entsprechend ITU-T-Empfehlung G.711 ist. Trifft dies zu, ist in der Subadresse, in der bereits die Zuordnungsnummer in den Oktetts 4

und 5 übertragen wird, im Oktett 6 das niederwertigste Bit (Bit 0) auf den Wert 1 zu setzen (siehe Anlage B.3.1). In allen anderen Fällen, d. h. bei Datenübertragung oder Anforderung einer transparenten Verbindung durch den züA, ist das Bit 0 des Oktetts 6 auf den Wert 0 zu setzen.

Im Normalfall ist in der Verbindung zur bS im Informationselement ‘Calling Party Subaddress’ die Rufnummer des züA zu übermitteln: In Oktett 4 der Subadresse ist das Oktett 3 des ‘Calling Party Number’ Informationselementes gemäß EN 300 403-1 [6] zu übertragen, d. h. die Information über ‘Type of Number’ und ‘Numbering Plan Identification’. Ab Oktett 5 sind in jeweils einem Halb-byte die einzelnen Ziffern (hexadezimal) der Rufnummer zu übertragen (siehe auch Anlage B.3.2).

Anlage B.1.3 Übermittlung der Ereignisdaten

Für jedes Ereignis gemäß § 7 TKÜV wird ein Datensatz gemäß Anlage B.2 an die bS gesendet. Ggf. können mehrere gleichartige Ereignisse (z. B. bei sequentieller Wahl) zusammengefasst und dann in einem Datensatz übertragen werden. Die Initiative für das Senden geht von der TKA-V aus.

Insbesondere ist bei Beginn und Ende der zu überwachenden Telekommunikation sowie bei jedem Ereignis gemäß § 7 TKÜV während der Telekommunikation (z. B. Aktivitäten im Rahmen eines Dienstmerkmals) ein Ereignisdatensatz zu übermitteln, der die relevanten in Anlage B.2 aufgeführten Daten enthält. Die Datensätze sind zeitnah, d. h. unverzüglich nach Auftreten des entsprechenden Ereignisses, zu übermitteln.

Für die Übermittlung der Datensätze stehen die Möglichkeiten nach Anlage A.1 zur Verfügung:

Anlage B.1.4 Keine Übermittlung von Informationen zur TKA-V

Nutz- oder Zeichengabesignale auf der Verbindung von der TKA-V zur bS dürfen keine Rückwirkungen auf die zu überwachende Telekommunikation haben.

Nach erfolgtem Aufbau der Verbindung von der TKA-V zur bS werden von den technischen Einrichtungen der bS keine Signale mehr zu den Anschlüssen der TKA-V übertragen. Dies gilt nicht für Quittungssignale (in Rückwärtsrichtung) als Bestandteil der Übertragungsprotokolle aller Schichten (z. B. X.25 [20], X.31 [1], FTAM [17], FTP) bei der Übermittlung von Ereignisdaten.

Für den paketvermittelnden Übergabepunkt gelten die vorstehenden Regelungen sinngemäß.

Authentifizierung bei der TKA-V

Für jede Überwachungsmaßnahme wird von der bS eine Zielrufnummer vergeben. Zur Authentifizierung werden Funktionen des DM COLP entsprechend ETS 300 094 [5] benutzt:

Bei teilnehmergleicher Anschaltung nutzt die TKA-V das DM COLP entsprechend ETS 300 094. Bei netzgleicher Anschaltung ist in der Zeichengabenachricht für die Anforderung zum Verbindungsaufbau zur bS die Rufnummer des Gerufenen anzufordern.

Vom Endgerät der bS wird das DM COLP unterstützt, indem es seine einprogrammierte Kennung, die jeweils der individuellen Rufnummer der Überwachungsmaßnahme (im allgemeinen eine MSN oder eine Anschlussnummer + Nebenstelle einer DDI) entspricht, in die Zeichengabenachricht für die Verbindungsannahme einfügt.

Die vom Endgerät gesendete Rufnummer wird vom Netz überprüft und erhält das Attribut ‘user provided, verified and passed’.

Die TKA-V vergleicht ihre für den Verbindungsaufbau verwendete individuelle Zielrufnummer mit der in der Zeichengabenachricht für die Verbindungsannahme (CONNECT) enthaltenen Rufnummer des Endgerätes der bS.

Stimmen beide überein, darf der Verbindungsaufbau fortgesetzt werden.

Stimmen sie **nicht** überein oder ist keine Rufnummer des Gerufenen vorhanden, ist die Verbindung unverzüglich von der TKA-V auszulösen.

Verläuft diese Authentifizierung zu irgendeinem Zeitpunkt negativ, erfolgen im Abstand von je 5 bis 10 Sekunden drei weitere Verbindungsaufbauversuche. Wenn auch beim letzten Verbindungsaufbauversuch die Authentifizierung nicht erfolgreich ist, ist die jeweilige Verbindung zur bS umgehend abzubrechen und in der TKA-V eine Fehlerbehandlung nach Anlage A.4 einzuleiten.

Auf Grund der Tatsache, dass die Connected Number nicht in jedem Fall von den beteiligten Netzen übermittelt wird, muss es der TKA-V möglich sein, den COLP-Check für eine individuelle Maßnahme zu deaktivieren. Kann der COLP-Check, insbesondere bei neueren Netztechnologien, nicht immer zuverlässig durchgeführt werden, kann dieser nach Rücksprache mit der Bundesnetzagentur dauerhaft deaktiviert werden.

Weiterhin müssen beim COLP-Check auch zwei unterschiedliche Nummern als gültig akzeptiert werden, nämlich die 'user provided number' und die 'network provided number'. Üblicherweise enthält die 'user provided number' eine DDI-Erweiterung.

Das Routing zu den Zieladressen der bSn muss derart erfolgen, dass die genannten Dienstmerkmale sicher übermittelt werden. Durch die Bereitstellung der Zieladressen der bSn durch die BNetzA muss ein Routing eingestellt werden, welches nur diesbezüglich „sichere“ Transitnetze berücksichtigt und etwa „unsichere“ IP-Netze bzw. weiterreichende ausländische Netze vermeidet.

Authentifizierung bei der berechtigten Stelle

Die technische Einrichtung der bS überprüft, ob die Rufnummer der TKA-V (Anschlussnummer an das Transitnetz), die im Informationselement ‘Calling Party Number’ übertragen wird, gültig ist. Daher darf die TKA-V zum Aufbau der Verbindungen zur bS nicht das Dienstmerkmal ‘Calling Line Identification Restriction’ nach ETS 300 090 [4] benutzen.

Da die TKA-V insbesondere bei Mobilfunknetzen für eine Überwachungsmaßnahme unterschiedliche Zugänge zum Transitnetz nutzen kann, muss bei der bS für eine Überwachungsmaßnahme u. U. eine Liste mit mehreren Rufnummern zur Authentifizierung eingerichtet werden.

Schutz vor Fehlverbindungen und Blockade

Es ist zu verhindern, dass unberechtigte Benutzer die Einrichtungen bei der bS anwählen können und deren Anschluss stören oder blockieren oder überwachten Verkehr simulieren. Außerdem muss sichergestellt werden, dass überwachte Telekommunikation nur zu den dazu vorgesehenen Anschlüssen der bS übermittelt werden kann.

Diese Forderungen werden durch Nutzung von Funktionen des Dienstmerkmals Closed User Group gemäß ETS 300 136 [9] bzw. X.25 erreicht. Hierzu wird einmalig je Netztyp des Transitnetzes (d. h. für das ISDN und paketvermittelnde Netze) eine Geschlossene Benutzergruppe - Closed User Group (CUG) - eingerichtet, die für alle Überwachungsmaßnahmen anzuwenden ist.

Die TKA-V nutzt bei teilnehmergleicher Anschaltung das Dienstmerkmal CUG entsprechend ETS 300 136 bzw. X.25 mit der Option ‘incoming access not allowed’ und ‘outgoing access not allowed’, bei netzgleicher Anschaltung (entfällt bei X.25) ist in die Zeichengabenachricht für die Anforderung zum Verbindungsaufbau der für die CUG festgelegte Interlock-Code einzusetzen, sowie für den CUG Call Indicator der Wert ‘CUG call without outgoing access’.

Anlage B.2 Der Datensatz

Die Informationen über die beim züA auftretenden Ereignisse werden als Datensätze zeitnah in Bezug auf die Übermittlung der Nutzinformationen an die bS übermittelt. Solche Ereignisse sind z. B. Beginn und Ende einer Verbindung, aber auch im Falle

- nicht rufbezogener Ereignisse,
- wenn der Verbindungsaufbau vom züA zu seinem Telekommunikationspartner oder umgekehrt abgebrochen wird oder nicht zustande kommt,

sind Datensätze mit den entsprechenden Informationen an die bS zu senden.

Erläuterung der Abkürzungen in den nachfolgenden Beschreibungen der Datensätze:

m = mandatory

c = conditional

Anmerkung: Conditional bedeutet, dass dieser Parameter zu der bS zu übermitteln ist, wenn dieser für die Überwachungsmaßnahme relevant ist.

Der Inhalt der Datensätze ist der bS im Klartext zu übermitteln. Als Zeichensatz ist der Zeichensatz nach ISO 8859-1 zu verwenden.

Neben der Übermittlung der Ereignisdaten im Klartext darf ein Kodierungsschema für die Ereignisdaten nur angewendet werden, wenn dieses mit der Bundesnetzagentur abgestimmt ist. Das Kodierungsschema muss für die komplette TKA-V gelten. Die Struktur des Datensatzes (siehe Anlage B.2.1) bleibt hiervon unberührt.

Der Datensatz hat kein einheitliches Format, er kann je nach vorliegendem Informationsgehalt aus einem oder mehreren der nachstehend aufgeführten Feldern zusammengesetzt sein. Wenn z. B. das Beginndatum einer zu überwachenden Telekommunikation im ersten Datensatz übertragen wurde, kann in den nachfolgenden Datensätzen dieses Feld entweder leer bleiben oder auch entfallen. Die Bezeichnung der Felder und der Inhalt müssen jedoch den Vorgaben entsprechen.

Bei mehreren Einträgen in einem Feld (mehrere Parameter) sind diese durch das Zeichen ASCII 35 (#) zu trennen.

Die Feldbezeichnung besteht aus einer 3-stelligen Nummer und optional der Bezeichnung, die in eckige Klammern gesetzt sind. Ab der nächsten Zeile sind dann die Parameter zu schreiben.

Beispiel:

[001: Versionskennung]

xyz

[002: Datensatzkennung]

D2#AA#05/08/96 11:26:15

[003: Datensatzart]

Beginn

[004: Referenznummer]

06131181166

[005: Zuordnungsnummer]

367.....

Anlage B.2.1 Struktur des Datensatzes

Die Felder der Datensätze sind nachstehend aufgelistet:

Feldbezeichnung	Bed.	Erläuterung
[001: Versionskennung]	m	
[002: Datensatzkennung]	m	
[003: Datensatzart]	c	Beginn, Ende, Continue, Report
[004: Referenznummer]	m	Kennzeichnungsmerkmal der Überwachungsmaßnahme gemäß § 7 Abs. 2 Satz 1 TKÜV
[005: Zuordnungsnummer]	c	Nummer für die Verbindung innerhalb einer Überwachungsmaßnahme, sie dient der Zuordnung des Datensatzes zu der Nutzinformation gemäß § 7 Abs. 2 Satz 2 TKÜV (nicht beim Report-Datensatz)
[006: Kennung des züA]	m	gemäß § 7 Abs. 1 Satz 1 Nr. 1 TKÜV
[007: Partner-Kennung]	c	gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV die Adressen der anderen Anschlüsse (wenn unvollständig nur die gewählten Ziffern) Bedingung: Wenn bekannt, ansonsten die bisher gewählten Ziffern
[008: Beginn]	c	Beginn der zu überwachenden Telekommunikation Bedingung: § 7 Abs. 1 Satz 1 Nr. 8 TKÜV
[009: Ende]	c	Ende der zu überwachenden Telekommunikation Bedingung: § 7 Abs. 1 Satz 1 Nr. 8 TKÜV
[010: Dauer]	c	Dauer der zu überwachenden Telekommunikation Bedingung: § 7 Abs. 1 Satz 1 Nr. 8 TKÜV
[011: Richtung]	c	Richtung der Telekommunikation, gehend oder kommend, bezogen auf den züA (§ 9 Abs. 2 Satz 1 Nr. 5 TKÜV) nicht relevant für Report-Datensätze, ausgenommen bei E-Mail
[012: Dienst]	c	Bearer- oder Teleservice (§ 7 Abs. 1 Satz 1 Nr. 5 TKÜV)
[013: Dienstmerkmal]	c	Bedingung: Falls vorhanden (§ 7 Abs. 1 Satz 1 Nr. 5 TKÜV)
[014: Benutzerdaten]	c	Bedingung: Falls vorhanden
[015: Standortangabe]	c	Bedingung: bei Mobilfunknetzen mandatory (§ 7 Abs. 1 Satz 1 Nr. 7 TKÜV)
[016: Rufzonenkennung]	c	Kennung nach § 7 Abs. 1 Satz 1 Nr. 7 TKÜV
[017: Funkrufnachricht]	c	
[018: Auslösegrund-züA]	c	Bedingung: Falls vorhanden (§ 7 Abs. 1 Satz 1 Nr. 6 TKÜV)
[019: Auslösegrund-Stich]	c	Bedingung: Falls vorhanden
[020: Beginn-ÜM]	m	Einmalig je Überwachungsmaßnahme (§ 5 Abs. 5 TKÜV)
[021: Ende-ÜM]	m	Einmalig je Überwachungsmaßnahme (§ 5 Abs. 5 TKÜV)

Tabelle Anlage B.2-1 Struktur und Inhalt der Ereignisdatensätze

Anlage B.2.2 Parameter in den Ereignisdatensätzen

Die nachfolgenden Erläuterungen zu den Parametern in den Ereignisdatensätzen richten sich nach der Tabelle Anlage B.2-1 und ergänzen die entsprechenden Anforderungen der TKÜV.

Versionskennung

Dieses Feld enthält eine Kennung, die vom Betreiber der TKA-V vergeben wird und die jeweilige Version der Schnittstelle kennzeichnet.

Parameter:	**Versionskennung**
Kodierung:	ASCII
Inhalt:	Versionsbezeichnung (max. 20 Zeichen)

Datensatzkennung

Die Datensatzkennung setzt sich aus den Angaben 'Netzbetreiberkennung' + 'interne Kennung' + 'Zeitstempel' zusammen:

Parameter:	**Datensatzkennung**
Kodierung:	ASCII
Inhalt:	Netzbetreiberkennung (max. 10 Zeichen)#interne Kennung (max. 10 Zeichen)#TT/MM/JJ hh:mm:ss

Die Netzbetreiberkennung wird nach Absprache mit dem Betreiber der TKA-V durch die Bundesnetzagentur festgelegt.

Die interne Kennung wird vom Betreiber der TKA-V festgelegt. Erfolgt kein Eintrag, ist ein Leerzeichen (ASCII 20 h) einzusetzen.

Die Angaben für Datum und Zeit in jeder Datensatzkennung beziehen sich auf den Erstellungszeitpunkt des Datensatzes. Es ist die Zeit auf der Basis amtlicher Zeit anzugeben, die Abweichungen dürfen höchstens ± 9 Sekunden betragen.

Anmerkung: Die Datensatzkennung ist **nicht** der Dateiname nach Anlage A.1 und Anlage A.2.

Datensatzart

Ein Datensatz ‘Begin’ wird am Beginn, ein Datensatz ‘End’ am Ende einer Verbindung zur bS gesendet.

Ein Datensatz ‘Continue’ wird jeweils gesendet, wenn im Laufe einer Verbindung weitere Ereignisse entsprechend § 7 Abs. 1 TKÜV eintreten.

Ein Datensatz ‘Report’ wird in der Regel gesendet zur Übermittlung nicht rufbezogener Ereignisse (z. B. Aktivierung einer Anrufweiterschaltung durch den züA oder bei Ereignissen in Speichersystemen).

Parameter:	**Datensatzart**
Kodierung:	ASCII
Inhalt:	Begin, End, Continue, Report

Referenznummer

Die Referenznummer dient zur Unterscheidung der einzelnen Überwachungsmaßnahmen bei der bS. Sie ist ein neutrales Zuordnungskennzeichen im Format einer Rufnummer nach E.164.

Parameter:	**Referenznummer**
Kodierung:	ASCII
Inhalt:	Rufnummer entsprechend E.164 (leitungsvermittelt) bzw. Rufnummer entsprechend X.121 (paketvermittelt)

Zuordnungsnummer

Die Zuordnungsnummer ist die eindeutige Nummer einer Verbindung innerhalb einer bestimmten Überwachungsmaßnahme und muss sowohl beim Aufbau der Verbindungen zur Übermittlung der Kopie der Nutzinformationen in der Subadresse als auch in jedem Datensatz zur Übermittlung von Ereignisdaten enthalten sein. Die Zuordnungsnummer ist eine Zahl zwischen 1 und 65535. Sie dient der Zuordnung der Ereignisdaten zu einer individuellen Verbindung, z. B. einem bestimmten Gespräch.

Zusätzlich (optional) kann von der TKA-V eine weitere Nummer hinzugefügt werden (z. B. in Mobilfunknetzen die Kennung der MSC), die zusammen mit der Zuordnungsnummer die Eindeutigkeit garantiert. Diese zweite Nummer ist eine Zahl zwischen 0 und 65535. Wird von der TKA-V diese Variante genutzt, ist die zweite Nummer getrennt durch das Zeichen ‘#’ hinter die Zuordnungsnummer zu setzen.

Parameter:	**Zuordnungsnummer**
Kodierung:	ASCII
Inhalt:	Integer 1 .. 65535
Beispiel:	[005: Zuordnungsnummer] 54546#23

Kennung des züA

Das Feld ‘Kennung des züA’ enthält die Adressdaten des züA.

Die Überwachungsmaßnahmen erhalten in den Netzen den Status einer ‘override category’, d. h. die Rufnummern werden an die bS übermittelt, auch wenn z. B. der züA das DM ‘CLIR’ nutzt, um die Rufnummernanzeige zu unterdrücken.

Die Adresse enthält ggf. neben der Rufnummer auch eine Subadresse, die in einer neuen Zeile an die bS zu übermitteln ist.

Wenn in der Anordnung als Kennung des züA eine IMSI genannt ist, kann in den Datensätzen als Kennung des züA auch eine IMSI eingetragen werden (die maximale Länge einer IMSI beträgt 15 Ziffern).

Wenn in der Anordnung als Kennung des züA eine IMEI genannt ist, muss in den Datensätzen diese IMEI und grundsätzlich die jeweils zugeordnete MSISDN eingetragen werden.

In IP-basierten Netzen ist die Kennung des züA ggf. eine SIP-URL entsprechend RFC 3261 [28].

Parameter:	**Kennung des züA**
Kodierung:	ASCII
Inhalt:	Rufnummer + Rufnummernplan-Identifier + Type of number
Kodierung (SUB):	Kopie des SUB Information Elements nach EN 300 403-1, die Oktetts sind als hexadezimale Ziffern in einem ASCII-String zu kodieren

Beispiel für Rufnummern:	[006: Kennung des züA] 496131181166#E.164#international number SUB: 6C 04 80 XX XX XX ....
Beispiel für IMSI:	[006: Kennung des züA] 262931234567890#IMSI
Beispiel für IMEI:	[006: Kennung des züA] 449123456789012#IMEI 49171987654321#E.164#international number
Beispiel für SIP-URL:	[006: Kennung des züA] SIP-URL: (Textstring entsprechend RFC 2543)

Partner-Kennung

Das Feld ‘Partner-Kennung’ enthält die Adressdaten des vom züA angewählten Anschlusses bzw. des Anschlusses, der den züA angewählt hat. Im letzteren Fall kann diese Adresse nicht immer ermittelt werden, z. B. bei Interworking mit PSTN.

Die Überwachungsmaßnahmen erhalten in den Netzen jedoch den Status einer ‘override category’, d. h. die Rufnummern werden an die bS übermittelt, auch wenn z. B. der andere Anschluss das DM ‘CLIR’ nutzt, um die Rufnummernanzeige zu unterdrücken.

Die Adresse enthält ggf. neben der Rufnummer auch eine Subadresse, die in einer neuen Zeile an die bS zu übermitteln ist.

Parameter:	**Partner-Kennung**
Kodierung:	ASCII
Inhalt:	Rufnummer + Rufnummernplan-Identifier + Type of number+ Zusatzparameter
Kodierung (SUB):	Kopie des SUB Information Elements nach EN 300 403-1, die Oktetts sind als hexadezimale Ziffern in einem ASCII-String zu kodieren

Beispiel für Rufnummern:	[007: Partner-Adresse] 496131181166#E.164#international number#redirecting number SUB: 6C 04 80 XX XX XX ....

Beginn der zu überwachenden Telekommunikation

Hier ist der Beginn der zu überwachenden Telekommunikation anzugeben. Die Angabe erfolgt in der jeweiligen Systemzeit in der Form TT/MM/JJ hh:mm:ss.

Da sich die Angaben in diesem Feld auf die tatsächliche Telekommunikation des züA beziehen, können sie um wenige Sekunden von dem Zeitstempel in der Datensatzkennung abweichen.

Erläuterung: Nach § 7 Abs. 1 Satz 1 Nr. 8 TKÜV müssen mindestens zwei der drei nachfolgenden Daten an die bS übermittelt werden:

- Zeitpunkt des Beginns der Verbindung oder des Verbindungsversuches,
- Zeitpunkt des Endes der Verbindung oder des Verbindungsversuches,
- Dauer der Verbindung.

Wenn zwei der vorstehenden Daten übertragen werden, ist die Übermittlung des dritten Parameters optional.

Bei Report-Datensätzen ist das Datum nur in das Feld 'Beginn' einzutragen.

Parameter:	**Beginn der zu überwachenden Telekommunikation**
Kodierung:	ASCII
Inhalt:	TT/MM/JJ hh:mm:ss

Ende der zu überwachenden Telekommunikation

Hier ist das Ende der zu überwachenden Telekommunikation anzugeben. Die Angabe erfolgt in der jeweiligen Systemzeit in der Form TT/MM/JJ hh:mm:ss.

Da sich die Angaben in diesem Feld auf die tatsächliche Telekommunikation des züA beziehen, können sie um wenige Sekunden von dem Zeitstempel in der Datensatzkennung abweichen.

Erläuterung: Nach § 7 Abs. 1 Satz 1 Nr. 8 TKÜV müssen mindestens zwei der drei nachfolgenden Daten an die bS übermittelt werden:

- Zeitpunkt des Beginns der Verbindung oder des Verbindungsversuches,
- Zeitpunkt des Endes der Verbindung oder des Verbindungsversuches,
- Dauer der Verbindung.

Wenn zwei der vorstehenden Daten übertragen werden, ist die Übermittlung des dritten Parameters optional.

Parameter:	**Ende der zu überwachenden Telekommunikation**
Kodierung:	ASCII
Inhalt:	TT/MM/JJ hh:mm:ss

Dauer der zu überwachenden Telekommunikation

Hier ist die Dauer der zu überwachenden Telekommunikation anzugeben. Die Angabe erfolgt in der jeweiligen Systemzeit in der Form hh:mm:ss.

Da sich die Angaben in diesem Feld auf die tatsächliche Telekommunikation des züA beziehen, können sie um wenige Sekunden von dem Zeitstempel in der Datensatzkennung abweichen.

Erläuterung: Nach § 7 Abs. 1 Satz 1 Nr. 8 TKÜV müssen mindestens zwei der drei nachfolgenden Daten an die bS übermittelt werden:

- Zeitpunkt des Beginns der Verbindung oder des Verbindungsversuches,
- Zeitpunkt des Endes der Verbindung oder des Verbindungsversuches,
- **Dauer** der Verbindung.

Wenn zwei der vorstehenden Daten übertragen werden, ist die Übermittlung des dritten Parameters optional.

Parameter:	**Dauer der zu überwachenden Telekommunikation**
Kodierung:	ASCII
Inhalt:	hh:mm:ss

Richtung der Telekommunikation

Eindeutige Zuordnung, ob es sich um kommende oder gehende Telekommunikation bezogen auf den züA handelt.

Parameter:	**Richtung der Telekommunikation**
Kodierung:	ASCII
Inhalt:	gehend/kommend

Dienst

Eindeutige Kennung der angeforderten Dienste (Bearer- oder Teleservice) sowie den Dienst charakterisierende Parameter.

Der Datensatz enthält für jeden Dienst ein separates Feld.

Parameter:	**Dienst**
Kodierung:	ASCII
Inhalt:	a) BC, LLC, HLC (komplette Informationselemente (soweit vorhanden) in hexadezimaler Darstellung) b) Bezeichnung des Dienstes in Textform, z. B. speech BS 3,1k audio BS 64k UDI BS 3,1k Telephony TS 7 kHz telephony VT TS

	USBS

Beispiel:	[012: Dienst] BC: 04 03 80 90 A3 LLC: 7C 02 80 90 (LLC im Standard optional, daher nicht immer vorhanden) HLC: 7D 02 91 81 (HLC nur bei Telediensten vorhanden) 3,1k Telephony TS

Eine Liste mit den Bezeichnungen der derzeit bekannten standardisierten und nicht standardisierten Dienste ist in Anlage 4 enthalten. Weitere Dienste sind vom Betreiber der TKA-V in seinem Konzept zu beschreiben, sie werden (ohne Zuordnung zu einer TKA-V) in Anlage B.4 aufgenommen.

Dienstmerkmal (Supplementary Service)

Name oder eindeutige Kennung der angeforderten Dienstmerkmale sowie die das Dienstmerkmal charakterisierende Parameter.

Hierzu zählt z. B. das Umlenkziel einer aktivierten Anrufweiterschaltung.

Der Datensatz enthält für jedes Dienstmerkmal ein separates Feld.

Parameter:	**Dienstmerkmal (Supplementary Service)**
Kodierung:	ASCII
Inhalt:	CFU, CFB, CFNR, CD, ECT, CH, 3PTY, CONF …

Beispiel:	[013: Dienstmerkmal] CFU Umlenkziel: 496131181166#E.164#international number

Zugehörige Parameter sind in einer getrennten Zeile zu übermitteln.

Eine Liste mit den Bezeichnungen der derzeit bekannten standardisierten und nicht standardisierten Dienstmerkmale ist in Anlage B.4 enthalten. Weitere Dienstmerkmale sind vom Betreiber der TKA-V in seinem Konzept zu beschreiben, sie werden (ohne Zuordnung zu einer TKA-V) in Anlage B.4 aufgenommen.

Nutzdaten

Nachrichteninhalt von Statusmeldungen und ähnlichen Diensten (z. B. Daten des User to User Signalling Supplementary Service).

Soweit die Nutzdaten nach einer definierten (standardisierten) Tabelle vom Netz als Text kodiert werden, sind sie auch der bS als Text zu übermitteln. Werden transparente Daten übermittelt, deren Bedeutung dem Betreiber der TKA-V nicht bekannt ist, sind sie in hexadezimaler Darstellung an die bS zu übermitteln. Zur Unterscheidung ist entweder das Wort ‘Text:’ oder das Wort ‘Daten:’ voranzustellen.

Klartext kann nur verwendet werden, wenn der an die bS zu übertragende Text mit Zeichensatz UTF-8 kodiert werden kann. Ansonsten ist der Text in hexadezimaler Darstellung zu übertragen und die zugrunde liegende Zeichentabelle anzugeben.

Parameter:	**Nutzdaten**

Kodierung:	UTF-8
Inhalt:	Nutzdaten als Text oder in hexadezimaler Darstellung

Beispiel:	[014: Benutzerdaten] Text: Dies ist ein Beispieltext oder Daten:02 3F 4D 76 3A .... Zeichensatz: ETS 300 628 ‘default alphabet’

Zur Übermittlung des Nachrichteninhaltes eines Short Message Services muss jedoch immer der Inhalt der kompletten PDU (inkl. SM Header, User data header, User data) entsprechend der Spezifikation 3GPP TS 23.040 in hexadezimaler Form angegeben werden. Dies entspricht der Anforderung nach Anlage C bzw. D.

Standortangabe

Bei überwachten Anschlüssen von Mobilfunkteilnehmern ist der dem Netz bekannte Standort des Mobilfunkgerätes nach § 7 Abs. 1 Nr. 7 TKÜV mit der größtmöglichen Genauigkeit anzugeben.

Zur Umsetzung von Anordnungen, die Standortangaben von bereits empfangsbereiten Mobilfunkgeräten fordern, kann der hier beschriebene Datensatz ebenfalls verwendet werden.

Wird in dem Mobilfunknetz der Standort des Mobilfunkgerätes nicht erfasst, ist zumindest die Funkzelle anzugeben, über die die Verbindung abgewickelt wird. Die Zellenkennungen der Funkzellen, in die der züA während einer bestehenden Verbindung wechselt, sind nur insoweit an die bS zu übermitteln, wie sie gemäß der standardisierten Protokolle (MAP) zu der MSC übermittelt werden, von der aus die Verbindungen zur bS aufgebaut werden.

Die Standortangabe soll möglichst in einer Form kodiert werden, die es der bS ermöglicht, ohne netzspezifische Unterlagen des jeweiligen Netzbetreibers die geographische Lage der Funkzelle zu ermitteln.

Zu diesem Zweck sind zumindest die Koordinaten-Angaben des Standortes der jeweiligen Funkstelle (z. B. Base Transceiver Station im GSM oder Node B im UMTS) und die Zellenkennung CGI (Cell Global Identification, entsprechend ETS 300 523 [13]) anzugeben.

Als Standardwert für die Koordinaten-Angaben werden UTM-Ref-Koordinaten verwendet. Diese setzen sich aus Zonenfeld + 100 km Quadrat + Koordinate zusammen. Wird ein anderes Koordinatensystem verwendet, ist die Angabe des Koordinatensystems erforderlich (z. B. geografische Winkelkoordinaten).

Auf die Koordinaten-Angaben des Standortes kann verzichtet werden, wenn zusätzlich zur CGI eine Tabelle zur Umsetzung der Zellenkennung in eine geographische Lage verfügbar gemacht wird.

Hinweis: Im Rahmen der Implementierung nach den Anlagen C und D müssen beide Parameter berichtet werden.

Parameter:	**Standortangabe**
Kodierung:	ASCII
Inhalt:	Koordinatenangabe#Koordinatensystem und Zellenkennung

Beispiel für eine UTM-Ref-Koordinatenangabe mit CGI:	[015: Standortangabe] 32UMA43993966#UTM 262#07#C738#FF7C#CGI

Rufzonenkennung

Die Rufzone, in der die Nachricht ausgesendet wird.

Die Rufzonenkennung muss in einer Form kodiert werden, die es der bS ermöglicht, ohne netzspezifische Unterlagen des jeweiligen Netzbetreibers und ohne Rückfragen die geographische Lage der Rufzone zu ermitteln.

Zu diesem Zweck sind die Koordinaten-Angaben des Standortes des jeweiligen Funkrufsenders anzugeben.

Als Standardwert werden UTM-Ref-Koordinaten verwendet. Diese setzen sich aus Zonenfeld + 100 km Quadrat + Koordinate zusammen.

Wird ein anderes Koordinatensystem verwendet, ist die Angabe des Koordinatensystems erforderlich (z. B. geografische (Winkel)-Koordinaten).

Bei mehreren Rufzonen sind alle Koordinaten in getrennten Zeilen anzugeben.

Zusatzparameter sind hinter der Koordinate getrennt durch ein Doppelkreuz (#) einzutragen, z. B. Benennung der Rufzone(n) oder bei bundesweiter oder europaweiter Ausstrahlung ‘bw’ für bundesweit oder ‘ew’ für europaweit anzugeben. Die Angabe des Koordinatensystems ist nur erforderlich, wenn keine UTM-Ref-Koordinaten verwendet werden (z. B. geografische Winkelkoordinaten).

Parameter:	**Rufzonenkennung**
Kodierung:	ASCII
Inhalt:	Koordinatenangabe#Koordinatensystem#Zusatzparameter

Beispiel:	[016: Rufzonenkennung] 32UPA340756 oder 32UPA340756##bw

Die Genauigkeit ist abhängig von der Größe der Rufzone, die Abweichung darf ca. 10 % des jeweiligen Rufzonendurchmessers betragen.

Funkrufnachricht

Der von eventuell verwendeten Netzkodierungen befreite Inhalt der gesendeten Funknachrichten.

Parameter:	**Funkrufnachricht**
Kodierung:	ASCII
Inhalt:	Abhängig vom Dienst (siehe auch ETS 300 133-2 [8]) entweder • Angabe des gesendeten ‘urgent message indicator’ und des ‘alert signal indicator’ entsprechend ETS 300 133-4 [8] (Tone-only paging), • Angabe der gesendeten Ziffern (Numeric paging), • Angabe der gesendeten Zeichen (Alphanumeric paging) oder • Kopie der gesendeten Daten in hexadezimaler Darstellung (Transparent data paging).

Bei nicht standardisierten Funkrufdiensten sind die zur bS zu übermittelnden Nachrichten im vom Betreiber der TKA-V zu erstellenden Konzept zu beschreiben und mit der Bundesnetzagentur abzustimmen.

Auslösegrund – züA

Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde (entsprechend ETS 300 485 [12]).

Parameter:	**Auslösegrund - züA**
Kodierung:	ASCII
Inhalt:	a) Cause Information Element entsprechend ETS 300 485 in

	hexadezimaler Darstellung b) Text entsprechend ETS 300 485

Beispiel:	[018: Auslösegrund] cause ie:11 cause value: user busy

Auslösegrund – Stich

Angabe des Grundes, weshalb die Verbindung von der TKA-V zur bS (hier als Stich bezeichnet) nicht aufgebaut werden konnte oder ausgelöst wurde (Auslösegrund entsprechend ETS 300 485).

Parameter:	**Auslösegrund - Stich**
Kodierung:	ASCII
Inhalt:	a) Cause Information Element entsprechend ETS 300 485 in hexadezimaler Darstellung b) Text entsprechend ETS 300 485

Beispiel:	[019: Auslösegrund] cause ie:11 cause value: user busy

Beginn der Überwachungsmaßnahme

Mit dem Parameter Beginn-ÜM wird der bS angezeigt, dass die Überwachungsmaßnahme im Netz aktiviert wurde und von diesem Zeitpunkt an mit der Übermittlung von Ereignisdaten zu rechnen ist.

Parameter:	**Beginn der Überwachungsmaßnahme**
Kodierung:	ASCII
Inhalt:	TT/MM/JJ hh:mm:ss

Ende der Überwachungsmaßnahme

Mit dem Parameter Ende-ÜM wird der bS angezeigt, dass die Überwachungsmaßnahme im Netz deaktiviert wurde und von diesem Zeitpunkt an nicht mehr mit der Übermittlung von Ereignisdaten zu rechnen ist.

Parameter:	**Ende der Überwachungsmaßnahme**
Kodierung:	ASCII
Inhalt:	TT/MM/JJ hh:mm:ss

Anlage B.3 Verwendung der Subadressen

Nachfolgend werden die Verwendungen der folgenden Subadressen beschrieben:

1. ‘Called Party Subaddress’
2. ‘Calling Party Subaddress’
3. ‘Calling Party Subaddress’ bei Auslandskopfüberwachung

Anlage B.3.1: ‘Called Party Subaddress’

Verwendung des ‘Called Party Subaddress’-Informationsfeldes in dem Stich zur bS:

Bit Nr. ⇒	7	6	5	4	3	2	1	0	
Oktett Nr. ⇓									
1	Entsprechend Standard								
2	Entsprechend Standard								
3	Entsprechend Standard								
4	Zuordnungsnummer (niederwertiges Byte)								
5	Zuordnungsnummer (höherwertiges Byte)								
6	siehe unten								
7	Zusatznummer zur Zuordnungsnummer (niederwertiges Byte)								falls von der TKA-V eingefügt
8	Zusatznummer zur Zuordnungsnummer (höherwertiges Byte)								"
9									die nicht benutzten Oktetts sind
10									mit 'FF' hex zu füllen
11									oder abzuschneiden
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									

Oktett 6

7	6	5	4	3	2	1	0	< -- Bitposition
							0	= Daten transparent beim züA
							1	= Sprache/Audio, G.711 A-law
					0	0		= Richtung nicht relevant [1)]
					0	1		= Empfangsrichtung (Rx) beim züA
					1	0		= Senderichtung (Tx) beim züA

[1]Die Bezeichnung ‘Sende- oder Empfangsrichtung’ bezieht sich auf einen durchgeschalteten (B-)Kanal und ist nicht zu verwechseln mit der Richtung des Verbindungsaufbaus.

Anlage B.3.2: ‘Calling Party Subaddress’

Verwendung des ‘Calling Party Subaddress’-Informationsfeldes in den Stichen zur bS:

Bit Nr. ⇒	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
Oktett Nr. ⇓									
1	Entsprechend Standard								
2	Entsprechend Standard								
3	Entsprechend Standard								Oktett 3 des Calling Party Number Informationselementes entsprechend EN 300 403-1
4	Type of number				Numbering Plan identification				
5	2. Ziffer (hex)				1. Ziffer (hex)				Oktett 5 bis 14 enthält die Rufnummer des züA
6	4. Ziffer (hex)				3. Ziffer (hex)				die nicht benutzten Ziffern sind 'F' hex zu füllen oder
7	6. Ziffer (hex)				5. Ziffer (hex)				'0' bei gleichzeitiger Verwendung des odd/even indicators in Oktett 3
8	8. Ziffer (hex)				7. Ziffer (hex)				
9	10. Ziffer (hex)				9. Ziffer (hex)				
10	12. Ziffer (hex)				11. Ziffer (hex)				
11	14. Ziffer (hex)				13. Ziffer (hex)				
12	16. Ziffer (hex)				15. Ziffer (hex)				
13	18. Ziffer (hex)				17. Ziffer (hex)				
14	20. Ziffer (hex)				19. Ziffer (hex)				Nach EN 300 403-1 maximal 20 Zeichen
15									die nicht benutzten Oktetts sind
16									mit 'FF' hex zu füllen oder abzuschneiden
17									
18									
19									
20									
21									
22									
23									

Anlage B.3.3: ‘Calling Party Subaddress’ bei AKÜ

Bedingt durch die systembedingten Engpässe bei der Administrierung von Auslandskopf-Überwachungen nach § 4 Abs. 2 TKÜV in älteren Vermittlungsstellen (z.B. EWSD) sowie der Notwendigkeit von Mehrfachüberwachungen durch eine empfangende Stelle wird es notwendig, zukünftig die Referenznummer in der Subadresse übermitteln zu können. Diese Anpassung kann für alle älteren Vermittlungsstellen vorgenommen werden, auch wenn das verpflichtete Unternehmen selbst keine Auslandskopf-Vermittlungsstellen betreibt (siehe hierzu auch die Hinweise in Kapitel 3.2).

Verwendung des ‘Calling Party Subaddress’ Informationsfeldes in den Stichen zur bS:

Bit Nr. ⇒	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
Oktett Nr. ⇓									
1	Entsprechend Standard								
2	Entsprechend Standard								
3	Entsprechend Standard								Oktett 3 des Calling Party Number Informationselementes entsprechend EN 300 403-1
4	Type of number = ‚0’				Numbering Plan identification = ‚0’				Die Kodierung von Oktett 4 = ‚00’hex dient als Kennung, dass eine Referenznummer verwendet wird
5	2. Ziffer (hex)				1. Ziffer (hex)				Oktett 5 bis 14 enthält die Referenznummer der Maßnahme
6	4. Ziffer (hex)				3. Ziffer (hex)				Durch die Nutzung des Rufnummernschemas kann
7	6. Ziffer (hex)				5. Ziffer (hex)				maximal eine 20 stellige Referenznummer (anstatt
8	8. Ziffer (hex)				7. Ziffer (hex)				25 Stellen) genutzt werden.
9	10. Ziffer (hex)				9. Ziffer (hex)				
10	12. Ziffer (hex)				11. Ziffer (hex)				
11	14. Ziffer (hex)				13. Ziffer (hex)				
12	16. Ziffer (hex)				15. Ziffer (hex)				
13	18. Ziffer (hex)				17. Ziffer (hex)				
14	20. Ziffer (hex)				19. Ziffer (hex)				
15									Die nicht benutzten Oktetts sind
16									mit 'FF' hex zu füllen oder abzuschneiden
17									
18									
19									
20									
21									
22									
23									

Anlage B.4 Dienste und Dienstmerkmale

Die nachfolgenden Tabellen werden den Innovationszyklen der Telekommunikation entsprechend fortgeschrieben. Dienste und Dienstmerkmale, die nicht in den nachfolgenden Tabellen aufgeführt und nicht nach ETSI oder ITU-T standardisiert sind bzw. nicht nach diesen Standards realisiert werden sollen, müssen entsprechend im Konzept ausführlich beschrieben werden. Sie sind bezüglich der Relevanz zu Überwachungsmaßnahmen zu untersuchen. Grundsätzlich sind, wenn vom züA ein Dienst oder Dienstmerkmale in Anspruch genommen wird, die zugehörigen Informationen an die bSn zu übermitteln. Im Konzept ist vom Betreiber der TKA-V zu beschreiben, wie die Informationen in der TKA-V erfasst und an die bS übermittelt werden. Die Aussagen der Spalte 6, die die Relevanz zu den Überwachungsmaßnahmen beinhaltet, sind dabei zu berücksichtigen.

Bezeichnung 1	**Kurz-bezeichnung** 2	**ETS** 3	**ITU-REC** 4	**Kategorie** 5	**Relevanz zu Überwachungsmaßnahmen** 6
Circuit-mode 64 Kbit/s unrestricted, 8 kHz structured bearer service category	UDI BS	300 108	I.231.1	Circuit-mode bearer service categories	Unbedingt richtungsgetrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 64 Kbit/s, 8 kHz structured bearer service category usable for speech information transfer	speech BS	300 109	I.231.2	Circuit-mode bearer service categories	Richtungstrennung erforderlich, da Missbrauch möglich.
Circuit-mode 64 Kbit/s, 8 kHz structured bearer service category usable for 3.1 kHz audio information transfer	3,1k audio BS	300 110	I.231.3	Circuit-mode bearer service categories	Richtungstrennung erforderlich, da Missbrauch möglich. Bei Datenübertragung > 2,4 kbit/s (Modem), bei der dieser Bearer Service genutzt wird, besteht die technische Notwendigkeit der Richtungstrennung, da sonst die Signale bei der bS nicht reproduziert werden können.
Circuit-mode alternate speech / 64 Kbit/s unrestricted, 8 kHz structured bearer service category	alternate speech BS		I.231.4	Circuit-mode bearer service categories	Unbedingt richtungsgetrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 2x64 Kbit/s unrestricted, 8 kHz structured bearer service category	2x64k UDI BS		I.231.5	Circuit-mode bearer service categories	Unbedingt richtungsgetrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 384 Kbit/s unrestricted, 8 kHz structured bearer service category	384k UDI BS		I.231.6	Circuit-mode bearer service categories	Unbedingt richtungsgetrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 1536 Kbit/s unrestricted, 8 kHz structured bearer service category	1536k UDI BS		I.231.7	Circuit-mode bearer service categories	Unbedingt richtungsgetrennte Übermittlung der Nutzinformation erforderlich

Bezeichnung 1	**Kurz-bezeichnung** 2	**ETS** 3	**ITU-REC** 4	**Kategorie** 5	**Relevanz zu Überwachungsmaßnahmen** 6
ISDN Packet Mode Bearer Services; ISDN Virtual Call (VC) and Permanent Virtual Circuit Call (PVC) bearer services provided by the **B**-channel of the user access - basic and primary rate		300 048	I.232.1	Packet mode bearer service categories	
ISDN Packet Mode Bearer Services; ISDN Virtual Call (VC) and Permanent Virtual Circuit Call (PVC) bearer services provided by the **D**-channel of the user access - basic and primary rate		300 049	I.232.1	Packet mode bearer service categories	
User signalling bearer service category	USBS	300 716	I.232.3	Packet mode bearer service categories	
Frame relaying bearer service			I.233.1	Frame Mode bearer services	
ISDN Frame Relay Multicast Baseline Document			I.233.1	Frame Mode bearer services	
Telephony 3,1 kHz teleservice	3k Telephony TS	300 111	I.241.1	Teleservices	
Teletext teleservice	Teletext TS			Teleservices	
Service requirements for telefax group 4	FAX4 TS	300 120	I.241.3	Teleservices	
Mixed Mode teleservice	Mixed Mode TS		I.241.4	Teleservices	
Syntax-based Videotext teleservice	Videotext TS	300 262	I.241.5	Teleservices	
Telex teleservice	Telex TS		I.241.6	Teleservices	
Telephony 7 kHz teleservice	7k Telephony TS	300 263	I.241.7	Teleservices	
Teleaction	Teleaction		I.241.8	Teleservices	
Videotelephony teleservice	VT TS	300 264		Teleservices	
Eurofile transfer teleservice (EFT)	EFT TS	300 409 [11]		Teleservices	
File Transfer & Access Management teleservice (FTAM)	FTAM TS	300 410		Teleservices	

Tabelle Anlage B.4-1 Bearer und Teleservice

Bezeichnung 1	Kurz-bezeich-nung 2	ETS 3	ITU-REC 4	GSM 5	Kategorie 6	Relevanz zu Überwachungsmaßnahmen 7
Direct Dialling-In (DDI)	DDI	300 062	I.251.1		Address Information Supplementary Services	
Multiple Subscriber Number (MSN)	MSN	300 050	I.251.2		Address Information Supplementary Services	
Subaddressing Supplementary Service (SUB)	SUB	300 059	I.251.8		Address Information Supplementary Services	
Calling Line Identification Presentation (CLIP)	CLIP	300 089 300 514	I.251.3	02.04 02.81	Number Identification Supplementary Services	
Calling Line Identification Restriction (CLIR)	CLIR	300 090 300 514	I.251.4	02.04 02.81	Number Identification Supplementary Services	
PSTN-Calling Line Identification Presentation (CLIP)	PSTN CLIP				Number Identification Supplementary Services	
PSTN-Calling Line Identification Restriction (CLIR)	PSTN CLIR				Number Identification Supplementary Services	
Connected Line Identification Presentation (COLP)	COLP	300 094 300 514	I.251.5	02.04 02.81	Number Identification Supplementary Services	
Connected Line Identification Restriction (COLR)	COLR	300 095 300 514	I.251.6	02.04 02.81	Number Identification Supplementary Services	
Malicious Call Identification (MCID)	MCID	300 128	I.251.7	02.04	Call Registration Supplementary Services	
Calling Name Identification Presentation (CNIP)	CNIP		I.251.9		Name Identification Supplementary Services	
Calling Name Identification Restriction (CNIR)	CNIR		I.251.10		Name Identification Supplementary Services	
Call Forwarding Busy (CFB)	CFB	300 199 300 515	I.252.2	02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen

Bezeichnung	Kurz-bezeich-nung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Call Forwarding No Reply (CFNR)	CFNR	300 201	I.252.3	02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Forwarding Unconditional (CFU)	CFU	300 200 300 515	I.252.4	02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Forwarding on Mobile Subscriber Not reachable	CFNRc	300 515		02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Deflection (CD)	CD	300 202	I.252.5		Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Selective Call Forwarding (SCF)	SCF		I.252.8		Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Forwarding Unconditional to a Service Center (CFU-S)	CFU-S				Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Line Hunting (LH) Trunk Hunting (TH)	LH TH			02.04 (MAH)	Multiline Supplementary Services	
Call Waiting (CW)	CW	300 056 300 516	I.253.1	02.02 02.83	Call Completion Supplementary Services	
Completion of Calls to Busy Subscriber (CCBS)	CCBS	300 357	I.253.3	02.02	Call Completion Supplementary Services	
Completion of Calls on No Reply (CCNR)	CCNR		I.253.4		Call Completion Supplementary Services	
Conference Call, add-on (CONF)	CONF	300 183	I.254.1		Multiparty Supplementary Services	

Bezeichnung	Kurz-bezeich-nung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Multi-Party (MPTY)	MPTY	300 517		02.04 02.84	Multiparty Supplementary Services	
Three-Party (3PTY)	3PTY	300 186			Multiparty Supplementary Services	
Preset Conference Calling (PCC)	PCC		I.254.3		Multiparty Supplementary Services	
Conference, Booked add-on (BAC)	BAC		I.254.4		Multiparty Supplementary Services	
Meet-Me Conference (MMC)	MMC	300 164	I.254.5		Multiparty Supplementary Services	
Normal Call Transfer (NCT)	NCT		I.252.1		Multiparty Supplementary Services	
Explicit Call Transfer (ECT)	ECT	300 367	I.252.7	02.04	Multiparty Supplementary Services	Nach Transfer (Verbinden der beiden entfernten Partner) ist die Überwachung zu beenden.
Single-step Call Transfer (SCT)	SCT		I.252.8		Multiparty Supplementary Services	
Call Hold (HOLD)	HOLD	300 139 300 516	I.253.2	02.04 02.83	Multiparty Supplementary Services	
Closed User Group (CUG)	CUG	300 136 300 518	I.255.1	02.04 02.85	Community of Interest Supplementary Services	
Support of private numbering plans (SPNP)	SPNP		I.255.2		Community of Interest Supplementary Services	
Multi-Level Precedence and Preemption Service (MLPP)	MLPP		I.255.3		Priority Supplementary Services	
Priority Service	Priority		I.255.4		Priority Supplementary Services	
Outgoing Call Barring - User controlled	OCB-UC			02.04 02.88	Call Barring Supplementary Services	
Outgoing Call Barring - Fixed	OCB-F		I.255.5		Call Barring Supplementary Services	
Incoming Call Barring	BAIC		I.255.5	02.04 02.88	Call Barring Supplementary Services	

Bezeichnung	Kurz-bezeich-nung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Charge Card Calling (CCC)	CCC		E.116		Payment Changing Supplementary Services	
Virtual Card Calling (VCC)	VCC		E.116		Payment Changing Supplementary Services	
Credit Card Calling (CRED)	CRED		I.256.1		Payment Changing Supplementary Services	
Advice of charge: charging information at call setup time (AOC-S)	AOC-S	300 178 300 519	I.256.2a	02.02 02.86	Advice of Charge Supplementary Services	
Advice of charge: charging information during the call (AOC-D)	AOC-D	300 179 300 519	I.256.2b	02.02 02.86	Advice of Charge Supplementary Services	Keine Übermittlung der (emulierten) Gebührenimpulse
Advice of charge: charging information at the end of the call (AOC-E)	AOC-E	300 180 300 519	I.256.2c	02.02 02.86	Advice of Charge Supplementary Services	
Advice of charge: charging information on user request (AOC-R)	AOC-R				Advice of Charge Supplementary Services	
Reverse Charging (REV) REV at call setup time (REV-S)	REV REV-S		I.256.3	02.02	Changed Charging Supplementary Services	
Reverse Charging (REV) REV unconditional (REV-U)	REV REV-U				Changed Charging Supplementary Services	
Reverse Charging (REV) REV during the call (REV-D)	REV REV-D				Changed Charging Supplementary Services	
ISDN Freephone Service (FPH) and International Freephone Services (IFS)	FPH IFS	300 208	I.256.4 ISDN E.152 PSTN	02.02	Changed Charging Supplementary Services	
Home Country Direct (HCD)	HCD		E.HDC		Changed Charging Supplementary Services	
Premium Rate (PRM)	PRM	300 712			Changed Charging Supplementary Services	
User-to-User Signalling (UUS)	UUS	300 284	I.257.1	02.02	Additional Information Transfer Supplementary Services	

Bezeichnung 1	Kurz-bezeich-nung 2	ETS 3	ITU-REC 4	GSM 5	Kategorie 6	Relevanz zu Überwachungsmaßnahmen 7
Message Waiting Indication (MWI)	MWI				Additional Information Transfer Supplementary Services	
Terminal Portability (TP)	TP	300 053	I.258.1		Miscellaneous	
Incall Modification (IM)	IM		I.258.2		Miscellaneous	
Remote Control (RC)	RC		I.258.3		Help Supplementary Services	
Televoting (VOT)	VOT	300 713			Opinion Collection Supplementary Services	
Universal Access Number (UAN)	UAN	300 710			Numbering and Routing Supplementary Services	

Tabelle Anlage B.4-2 Supplementary Services

Bezeichnung der GSM-Telekommunikationsdienste in den Datensätzen

Die GSM-Telekommunikationsdienste sind in der Serie GSM 02.XX beschrieben.

1 Bearer Services

Wird vom züA ein ‘Bearer Service’ angefordert, ist bei der Übermittlung der Ereignisdaten im Feld ‘012: Dienst’ die Nummer des ‘Bearer Service’ entsprechend ETS 300 501 Table 2/GSM 02.02 anzugeben.

2 Teleservices

Wird vom züA ein ‘Teleservice’ angefordert, ist bei der Übermittlung der Ereignisdaten im Feld ‘012: Dienst’ die Nummer des Teleservices gemäß ETS 300 502 Table 2/GSM 02.03 anzugeben.

Beispiel:

Wird vom züA der Telefondienst angefordert, sind folgende Informationen zu übertragen:

[012: Dienst]

11

3 Supplementary Services

Wird vom züA ein ‘Supplementary Service’ in Anspruch genommen, ist bei der Übermittlung der Ereignisdaten im Feld ‘013: Dienstmerkmal’ die Kurzbezeichnung des Dienstmerkmals gemäß ETS 300 503 Table 4.1/GSM 02.04 anzugeben.

Beispiel:

Wird vom züA das Dienstmerkmal Hold angefordert, sind folgende Informationen zu übertragen:

[013: Dienstmerkmal]

02.83 2. HOLD

Anlage C Festlegungen für PSTN und ISDN (ETSI ES 201 671 bzw. TS 101 671)

Hinweis zur Nutzung bestehender Anlagen basierend auf Ausleitungen per ISDN oder X.25/X.31:

Aufgrund des mittelfristig absehbaren Abschaltens ISDN-basierter Technik muss auch die entsprechende Ausleitung, basierend auf dieser Technik, mittelfristig angepasst werden. Grundsätzlich sind neue Implementierungen, deren Ausleitung auf ISDN basiert, nicht mehr möglich. Bestehende Anlagen sind bis spätestens zum 31.12.2021 auf Ausleitungen nach Anlage D bzw. Anlage H umzustellen. Ist die Versorgung über den bestehenden Anbieter innerhalb dieser Frist nicht mehr möglich, so kann auch ein Wechsel zu einem alternativen Anbieter, der weiterhin ISDN anbietet, erfolgen. Zudem ist eine Vereinheitlichung der Schnittstellen vorgesehen: Aus diesem Grund sind bis zum 31.12.2017 alle Ausleitungen über X.25/X.31 durch Ausleitungen per FTP zu ersetzen.

Diese Anlage beschreibt die Bedingungen, wenn der Übergabepunkt für leitungsvermittelnde Festnetze (PSTN und ISDN) nach dem ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 [22] gestaltet wird. Der Übergabepunkt für Mobilfunknetze muss nach Anlage D erfolgen.

Hierzu gehört die Entscheidung über die im Standard bzw. in der Spezifikation enthaltenen Optionen und die Festlegung ergänzender technischer Anforderungen.

Grundsätzlich werden die Anforderungen für Datendienste im Mobilfunknetz aus der 3GPP-Spezifikation TS 33.108 in die ETSI-Spezifikation TS 101 671 übernommen. Sofern zur notwendigen Implementierung einer Überwachungslösung dies noch nicht erfolgt ist, muss deren Gestaltung mit der Bundesnetzagentur abgestimmt werden.

Im Teil A, Abschnitt 4.1 dieser TR TKÜV sind die Kennungen aufgelistet, auf Grund der die Überwachung der Telekommunikation umgesetzt werden muss. Wenn in der Anordnung als Kennung des züA eine IMEI genannt ist, muss in den Datensätzen diese IMEI und grundsätzlich die jeweils zugeordnete MSISDN eingetragen werden.

Neben den Anforderungen nach Teil A, Abschnitte 3 und 4, sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Kopie der Nutzinformation erfolgt bei PSTN, ISDN und GSM per ISDN-Doppelstiche und ist in dieser Anlage C beschrieben. Die Übermittlung der Ereignisdaten kann wahlweise per FTAM/X.25 oder FTP/Internet erfolgen. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten Die Übermittlung der Kopie der Nutzinformationen sowie der Ereignisdaten kann bei GPRS wahlweise per FTP oder TCP/IP erfolgen. Bei der Übermittlung per FTP/Internet gilt ebenfalls diese Anlage
Anlage A.2	Teilnahme am VPN mittels Kryptobox Wird die Übermittlung der Kopie der Nutzinformation bzw. der Ereignisdaten per FTP oder TCP/IP vorgenommen, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern

Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage C.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Die nachfolgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 101 671 bzw. des ETSI-Standards 201 671 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich die Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation bzw. des ETSI-Standards:

Abschnitt ES 201 671 / TS 101 671	**Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
5.1	**Manual/Electronic Handover Interface 1 (HI1)** Ein elektronisches Interface von der LEA zur Anlage des Verpflichteten zur direkten Administration von Maßnahmen wird nicht eingesetzt. Die Ereignisse zur Administrierung einer Maßnahme (z.B. über die Aktivierung) sowie Fehlermeldungen sind zu berichten.	Zur Übermittlung von Ereignissen (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme, Fehlermeldungen) von der Anlage des Verpflichteten zur LEA kann das HI1 eingesetzt werden (siehe hierzu Anlage A.3 der TR TKÜV).
6.2.1	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen NWO/AP/SvP-identifier (Operator Identifier). In Deutschland werden die ersten Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
8.1	**Data transmission protocol (HI2)** Zur Übermittlung der Ereignisdaten (IRI) über das HI1- und HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig. Die FTP-Verbindung ist sofort nach Übermittlung der Ereignisdaten auszulösen.	Zur Übermittlung dieser Ereignisdaten (HI1 und HI2) steht alternativ die Übermittlungsmethode nach Anlage B (X.25) zur Auswahl (siehe auch Anlage A.3 der TR TKÜV).
10.1	**Timing (Buffering of IRI)** Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	siehe Anlage A.4 der TR TKÜV.
11	**Security aspects** Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet. Bei Übermittlung der Nutzinformationen über ISDN werden die Dienstmerkmale CLIP, COLP und CUG genutzt.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Anlage A2 der TR TKÜV vorgesehen. Kann der COLP-Check, insbesondere bei neueren Netztechnologien, nicht immer zuverlässig durchgeführt werden, kann dieser nach Rücksprache mit der Bundesnetzagentur dauerhaft deaktiviert bzw. muss nicht implementiert werden.
12	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜV.	
Annex A: Circuit switched network handover		
A.1.3	**Usage of Identifiers** Die Optionen 'IRI and CC' und 'only IRI' müssen unterstützt werden; die Option 'only CC' muss nicht unterstützt werden.	Die Option 'only CC' ist bis zur Version 2.5.1 der Spezifikation enthalten.

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
A.3.2.1	**Control information for HI2** Alle Zeiten (TimeStamp) sind generell als local time auf Basis der gesetzlichen Zeit anzugeben.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*.
A.4.1	**Delivery of Content of Communication** Zur Korrelation der Nutzinformationen (CC) zu den anderen HI-Interfaces wird nicht der User-to-User Service, sondern der Subaddress Service genutzt.	Da der User-to-User Service in Deutschland nicht in allen Netzen implementiert ist, wird ausschließlich die Korrelation durch die Subadresse durchgeführt. Im Annex E ist diese Nutzung beschrieben.
A.4.2	**Delivery of packetized Content of Communication** Bei den Diensten SMS und UUS werden die Nutzinformationen als Ereignisdaten übermittelt.	Zur Übermittlung dieser Nutzinformationen kann wahlweise das ASN.1-Modul 'HI2Operations' nach Annex D.5 oder das Modul ' HI3CircuitDataOperations' nach Annex D.6 genutzt werden. In beiden Modulen sind entsprechende Parameter für UUS und SMS vorgesehen.
A.4.3	**Control information for circuit switched Content of Communication** Wie beschrieben, antworten die Endeinrichtungen der bSn auf eine SETUP-Nachricht sofort mit einer CONNECT-Nachricht, d. h. ohne eine ALERTING-Nachricht.	
A.4.4.1	**Failure of CC links** Bei erfolglosem Verbindungsaufbau müssen drei Wiederholversuche durchgeführt werden.	siehe Anlage A.4 der TR TKÜV.
A.4.4.2	**Fault Reporting** Fehlermeldungen werden als Ereignisdaten gemäß Annex D.5 (IRI) übermittelt (siehe Anlage A.4 der TR TKÜV). In Mobilfunknetzen sind die Angaben über Störungen, die sich nur in regional begrenzten Bereichen des Netzes auswirken, nur auf Nachfrage der berechtigten Stelle zu machen.	Die Fehlermeldungen können alternativ als nationale Parameter oder mittels des HI1-Interfaces übermittelt werden. Die zumindest zu übermittelnden Fehlerereignisse richten sich nach den Festlegungen der nationalen Parameter (siehe Anlage A.3 der TR TKÜV).
A.4.5	**Security Requirements at the interface port HI3** Beim Aufbau der CC links zur LEMF (LEA) müssen die ISDN-Dienstmerkmale CLIP, COLP und CUG genutzt werden. Das Routing zu den Zieladressen der bSn muss derart erfolgen, dass die genannten Dienstmerkmale sicher übermittelt werden.	Kann der COLP-Check, insbesondere bei neueren Netztechnologien, nicht immer zuverlässig durchgeführt werden, kann dieser nach Rücksprache mit der Bundesnetzagentur dauerhaft deaktiviert bzw. muss nicht implementiert werden. Durch die Bereitstellung der Zieladressen der bSn durch die BNetzA muss ein Routing eingestellt werden, welches nur diesbezüglich „sichere“ Transitnetze berücksichtigt und etwa „unsichere“ IP-Netze bzw. weiterreichende ausländische Netze vermeidet.

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
A.4.5.3	**Authentication** Eine besondere Authentisierungsprozedur im ISDN-B-Kanal oder in den Subadressen wird nicht genutzt.	
A.5	**LI procedures for circuit switched supplementary services** Für nicht standardisierte (proprietäre) überwachungsrelevante Dienstmerkmale müssen die notwendigen Informationen in den nationalen Parametern übermittelt werden. Die Inhalte der Parameter müssen mit der Bundesnetzagentur abgestimmt werden.	
A.5.4 A.6.11 A.6.2, A.6.3, A.6.12	**Multi party calls – general principles** Bei der großen Konferenz (CONF) für mehr als sechs Teilnehmer muss die Option B nach A.5.4.2 realisiert werden. Bei CW, HOLD, 3PTY und CONF bis sechs Teilnehmer kann alternativ Option A oder Option B genutzt werden.	Für CW, HOLD, 3PTY und CONF bis sechs Teilnehmer gilt: Da die Mehrfachnutzung der ISDN-Kanäle zur berechtigten Stelle nach Option B eine komplexere Zuordnung sowie eine erschwerte Auswertung der Nutzinformationen (keine Sprecherdifferenzierung per Kanal) bedingt, soll bevorzugt Option A implementiert werden.
A.6.3	**Call Hold/Retrieve** Bei Aktivierung von HOLD müssen beide CC links während der HOLD-Phase stumm geschaltet werden. Darüber hinaus wird die Option akzeptiert, bei der nur die gehaltene Kennung (held party) stumm geschaltet wird.	
A.5.5	**Subscriber Controlled Input** Bei Registrierungs- und Aktivierungsvorgängen sind Ereignisdaten auch dann zu erzeugen, wenn die Steuerung von Betriebsmöglichkeiten auf indirektem Weg (z.B. über eine Servicenummer oder per Webzugriff) geschieht.	Diese Forderung richtet sich nach § 5 Abs. 1 Nr. 4 TKÜV. Die jeweiligen Ereignisse und zugehörigen Daten sind mit der Bundesnetzagentur im Einzelfall abzustimmen.
A.6.4	**Explicit Call Transfer (ECT)** Nach dem Transfer muss die Option 2 realisiert werden ("The transferred call shall not be intercepted.").	
A.6.22	**User-to-User Signalling (UUS)** Die Nutzinformationen des Dienstes UUS werden als Ereignisdaten übermittelt.	Siehe Abschnitt A.4.2 dieser Tabelle.
A.8.3	**HI3 (delivery of CC)** Die Nutzinformationen des Dienstes SMS werden als Ereignisdaten übermittelt. Zur Korrelation der Nutzinformationen (CC) zu den anderen HI-Interfaces wird der Subaddress Service nach Annex E genutzt.	Siehe Abschnitt A.4.2 dieser Tabelle. Siehe Abschnitt A.4.1 dieser Tabelle.

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
Annex C: HI2 Delivery mechanisms and procedures		
C.1 / C.2	**ROSE / FTP** Zur Übermittlung der Ereignisdaten (IRI) über das HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig.	siehe Abschnitt 8.1 dieser Tabelle. Zur Übermittlung dieser Ereignisdaten (HI1 und HI2) steht alternativ die Übermittlungsmethode nach Anlage B (X.25) zur Auswahl (siehe auch Anlage A.1 der TR TKÜV).
C.2.2	**Usage of FTP** Es muss die 'File naming method B' genutzt werden. Zusätzlich gelten die Bestimmungen der Anlagen A.1 und A.2 der TR TKÜV.	
Annex D: Structure of data at the Handover Interface		
D.3 bis D.8	**ASN.1-Moduls** Bei Verwendung des FTP zur Übermittlung der IRI haben die ROSE-Operations in den Anhängen keine Relevanz und müssen nicht implementiert werden.	Da nicht alle Module fehlerfrei spezifiziert wurden bzw. nicht alle notwendigen Parameter enthalten, veröffentlicht die Bundesnetzagentur auf ihrer Homepage eine Liste derjenigen Module, die bei der Implementierung genutzt werden können (siehe auch Anlage X.4 der TR TKÜV).
Annex E: Use of sub-address and calling party number to carry correlation information		
E.3.2	**Field order and layout** Die Parameter für die Zuordnung von CC und IRI nach Table E.3.2 und E.3.3 sind entsprechend zu verwenden. Zudem ist in den Oktetts 17-23 der Called Party Subaddress (Table E.3.4 und E.3.6) als Unterscheidungskriterium zu den Subadressen nach den Festlegungen der Anlage B der TR TKÜV das feste Bitmuster '45 54 53 49 20 56 32' hex = ETSI V2' einzutragen.	Nach den rein nationalen Festlegungen für leitungsvermittelnde Netze (Anlage B) werden ebenfalls Subadressen genutzt, jedoch mit einer anderen Besetzung. Damit die Auswerteeinrichtung der bS eine Unterscheidung treffen kann, muss dieses Unterscheidungsmerkmal zwingend erfolgen.

Anlage C.2 Erläuterungen zu den ASN.1-Beschreibungen

Die Bundesnetzagentur informiert gemäß § 11 Satz 5 TKÜV auf ihrer Internetseite über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage C sind aus den verschiedenen Versionen des ETSI-Standards ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung von FTP als Übertragungsprotokoll sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die im Standard bzw. in der Spezifikation als ‚conditional' und ‚optional' bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen im Standard bzw. der Spezifikation oder nach Anlage C.1 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats „OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, z.B. ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder z.B. DDMMYYhhmm = 23.07.2002 10:35 h als ‚2307021035' H und nicht ‚3270200153'H)

Die Übermittlung administrativer Ereignisse (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme sowie Fehlermeldungen) sowie zusätzlicher Ereignisse (z.B. bezüglich herstellereigener Dienste) erfolgt nach Anlage A.3.

Anlage D Festlegungen für GSM, GPRS, UMTS- und LTE-Netze (3GPP TS 33.108)

Hinweis zur Nutzung bestehender Anlagen basierend auf Ausleitungen per ISDN:

Aufgrund des mittelfristig absehbaren Abschaltens ISDN-basierter Technik muss auch die entsprechende Ausleitung, basierend auf dieser Technik, mittelfristig angepasst werden. Grundsätzlich sind neue Implementierungen, deren Ausleitung auf ISDN basiert, nicht mehr möglich. Bestehende Anlagen sind bis spätestens zum 31.12.2021 auf Ausleitungen nach Anlage H umzustellen. Ist die Versorgung über den bestehenden Anbieter innerhalb dieser Frist nicht mehr möglich, so kann auch ein Wechsel zu einem alternativen Anbieter, der weiterhin ISDN anbietet, erfolgen.

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt für GSM, GPRS, UMTS- und LTE-Netze nach der 3GPP-Spezifikation TS 33.108 [23]. Die Spezifikation enthält grundsätzlich die technische Beschreibung für den leitungsvermittelnden und paketvermittelnden Bereich sowie für Multimediadienste.

Die Beschreibung des leitungsvermittelnden und paketvermittelnden Bereiches entspricht dabei grundsätzlich den Beschreibungen des ETSI-Standards ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 nach Anlage C. Dementsprechend gelten die gleichen Festlegungen zur Optionsauswahl und zu den ergänzenden Anforderungen.

Hierzu gehört die Entscheidung über die im Standard bzw. in der Spezifikation enthaltenen Optionen und die Festlegung ergänzender technischer Anforderungen.

Im Teil A, Abschnitt 4 dieser TR TKÜV sind die Kennungen aufgelistet, auf Grund der die Überwachung der Telekommunikation umgesetzt werden muss. Wenn in der Anordnung als Kennung des züA eine IMEI genannt ist, muss in den Datensätzen diese IMEI und grundsätzlich die jeweils zugeordnete MSISDN eingetragen werden.

Neben den Anforderungen nach Teil A, Abschnitte 3 und 4, sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Nutzinformation erfolgt im leitungsvermittelten Bereich per ISDN-Doppelstiche und ist in dieser Anlage D beschrieben. Die Übermittlung der Ereignisdaten (ASCII-Dateien) kann wahlweise per FTAM/X.25 oder FTP/IP erfolgen. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten. Die Übermittlung der Kopie der Nutzinformationen sowie der Ereignisdaten im paketvermittelten Bereich sowie bei den Multimediadiensten erfolgt per FTP/Internet oder TCP/IP. Bei der Übermittlung per FTP gilt ebenfalls diese Anlage.
Anlage A.2	Teilnahme am VPN mittels Kryptobox. Wird die Übermittlung per FTP bzw. TCP/IP über das Internet vorgenommen, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen

	Umsetzung von Überwachungsmaßnahmen

Anforderungen zur Standortangabe bei Mobilfunknetzen

Gemäß § 7 Abs. 1 Nr. 7 TKÜV sind bei einer zu überwachenden Kennung, deren Nutzung nicht ortsgebunden ist, Angaben zum Standort des Endgerätes mit der größtmöglichen Genauigkeit, die in dem das Endgerät versorgenden Netz für diesen Standort üblicherweise zur Verfügung steht zu berichten.
Zur Umsetzung von Anordnungen, durch die Angaben zum Standort des empfangsbereiten, der zu überwachenden Kennung zugeordneten Endgerätes verlangt werden, kann die vorzuhaltende Überwachungseinrichtung entsprechend genutzt werden.

Hierzu gelten folgende Festlegungen:

Die Standortangabe muss in einer Form kodiert werden, die es der bS ermöglicht, ohne netzspezifische Unterlagen des jeweiligen Netzbetreibers die geographische Lage der Funkzelle zu ermitteln.

Zu diesem Zweck sind die Koordinaten-Angaben des Standortes der jeweiligen Funkstelle (z. B. BTS im GSM, NodeB im UMTS oder eNodeB bei LTE) und die Zellenkennung CGI (Cell Global Identification, entsprechend ETS 300 523 [13]) bzw. die ECI (E-UTRAN Cell Identifier entsprechend ETSI TS 123 003) anzugeben.
Für die Koordinaten-Angaben müssen geographische Winkelkoordinaten auf Basis von WGS84 verwendet werden.

Wird in dem Mobilfunknetz der genaue Standort des Mobilfunkgerätes nicht erfasst, ist zumindest die Funkzelle anzugeben, über die die Verbindung abgewickelt wird.

Die Standortangabe bzw. die Zellenkennungen sind grundsätzlich zu berichten, auch wenn hierzu Informationen nicht im Kernnetz, sondern lediglich im Zugangsnetz vorliegen. Unter Berücksichtigung der von den Netzen bisher bereitstellbaren Funktionen müssen die Angaben zumindest bei den nachfolgenden Events berichtet werden:

- Circuit Switched Service
  Idle Mode: Periodic Location Update
  Connected Mode: Verbindungsauf und -abbau, Handover zwischen Zellen und SMS-Versand
- Data Service, 2.5G
  Standby Mode: Periodic Routing Area Update, Routing Area Update
  Ready Mode: GPRS-Attach und -Detach, Cell Updates (bei aktiviertem PDP Context) und Routing Area Update
- **Data Service, 3G**
  Idle Mode: Periodic Routing Area Update, Routing Area Update
  Connected Mode: GPRS-Attach und -Detach und Routing Area Update,
  Cell Updates (bei aktiviertem PDP Context im Modus CELL_DCH)~~, letzteres spätestens 1 Jahr nachdem eine entsprechende Erweiterung der Spezifikation 3GPP TS 33.108 veröffentlicht wurde~~
- **Data Service, 4G**
  Idle Mode: Periodic Tracking Area Update, Tracking Area Update
  Connected Mode: Attach und Detach, Tracking Area Update
  Inter-eNodeB-Handover~~, spätestens 1 Jahr nachdem eine entsprechende Erweiterung der Spezifikation 3GPP TS 33.108 veröffentlicht wurde.~~

Informativer Hinweis: Bei anderen bzw. künftigen Netzen (z.B. 5G) ist sicherzustellen, dass die im Gesamtnetz verfügbaren und bisher zur Verfügung gestellten Standortangaben auch dann berichtet werden, wenn die Standardisierung nicht berücksichtigt hat, diese Informationen zum Kernnetz bzw. zu den Erfassungspunkten der Ereignisdaten zu transportieren.

Anlage D.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Die nachfolgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP-Spezifikation TS 33.108 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation:

Abschnitt 3GPP TS 33.108	**Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
4.3	**Functional requirements** Die Optionen ‚IRI and CC' und ‚only IRI' müssen unterstützt werden; die Option ‚only CC' muss nicht unterstützt werden.	
4.4	**Overview of handover interface** Ein elektronisches Interface von der LEA zur Anlage des Verpflichteten zur direkten Administration von Maßnahmen wird nicht eingesetzt. Die Ereignisse zur Administrierung einer Maßnahme (z.B. über die Aktivierung) sowie Fehlermeldungen sind zu berichten.	Zur Übermittlung von Ereignissen (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme, Fehlermeldungen) von der Anlage des Verpflichteten zur LEA kann das HI1 eingesetzt werden (Anlage A.3 der TR TKÜV).
4.5	**HI2: Interface port for intercept related information** Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	siehe Anlage A.4 der TR TKÜV.
4.5.1	**Data transmission protocols (HI2)** Zur Übermittlung der Ereignisdaten (IRI) über das HI1- und HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig. Die FTP-Verbindung ist sofort nach Übermittlung der Ereignisdaten auszulösen.	Zur Übermittlung dieser Ereignisdaten (HI1 und HI2) steht alternativ die Übermittlungsmethode nach Anlage B (X.25) zur Auswahl (Anlage A.3 der TR TKÜV).
Ergänzung 1	**Security aspects** Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet. Bei Übermittlung der Nutzinformationen über ISDN werden die Dienstmerkmale CLIP, COLP und CUG genutzt.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Anlage A2 der TR TKÜV vorgesehen. Kann der COLP-Check, insbesondere bei neueren Netztechnologien, nicht immer zuverlässig durchgeführt werden, kann dieser nach Rücksprache mit der Bundesnetzagentur dauerhaft deaktiviert bzw. muss nicht implementiert werden.
Ergänzung 2	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜV.	

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
Ergänzung 3	**Failure of CC links** Bei erfolglosem Verbindungsaufbau müssen drei Wiederholversuche durchgeführt werden.	siehe Anlage A.4 der TR TKÜV.
Chapter 5: Circuit-switch domain		
5.1.2.1	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen Operator – (NO/AN/SP) identifier. In Deutschland werden die ersten Stellen auf ‚49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
5.2.2.1	**Control Information for HI2** Alle Zeiten (TimeStamp) sind generell als local time auf Basis der gesetzlichen Zeit anzugeben.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*.
5.3.1 5.3.1, 5.4	**Delivery of Content of Communication** Zur Korrelation der Nutzinformationen (CC) zu den anderen HI-Interfaces wird nicht der User-to-User Service, sondern der Subaddress Service genutzt. Bei den Diensten SMS und UUS werden die Nutzinformationen als Ereignisdaten übermittelt.	Da der User-to-User Service in Deutschland nicht in allen Netzen implementiert ist, wird ausschließlich die Korrelation durch die Subadresse durchgeführt. Im Annex E ist diese Nutzung beschrieben. Zur Übermittlung dieser Nutzinformationen kann wahlweise das ASN.1-Modul ‚HI2Operations' nach Annex D.5 oder das Modul, HI3CircuitDataOperations' nach Annex D.6 genutzt werden. In beiden Modulen sind entsprechende Parameter für UUS und SMS vorgesehen.
5.3.2	**Control information for Content of Communication** Wie beschrieben, antworten die Endeinrichtungen der bSn auf eine SETUP-Nachricht sofort mit einer CONNECT-Nachricht, d. h. ohne eine ALERTING-Nachricht.	
Ergänzung 4	**Fault Reporting** Fehlermeldungen werden als Ereignisdaten (IRI) übermittelt (siehe Anlage A.4 der TR TKÜV). In Mobilfunknetzen sind die Angaben über Störungen, die sich nur in regional begrenzten Bereichen des Netzes auswirken, nur auf Nachfrage der berechtigten Stelle zu machen.	Die Fehlermeldungen können alternativ als nationale Parameter oder mittels des HI1-Interfaces übermittelt werden. Die zumindest zu übermittelnden Fehlerereignisse richten sich nach den Festlegungen der nationalen Parameter (siehe Anlage A.3 der TR TKÜV).

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.3.3	**Security requirements at the interface port of HI3** Beim Aufbau der CC links zur LEMF (LEA) müssen die ISDN-Dienstmerkmale CLIP, COLP und CUG genutzt werden.	Kann der COLP-Check, insbesondere bei neueren Netztechnologien, nicht immer zuverlässig durchgeführt werden, kann dieser nach Rücksprache mit der Bundesnetzagentur dauerhaft deaktiviert bzw. muss nicht implementiert werden.
5.3.3.3	**Authentication** Eine besondere Authentisierungsprozedur im ISDN-B-Kanal oder in den Subadressen wird nicht genutzt.	
5.4	**LI procedures for supplementary services** Für nicht standardisierte (proprietäre) überwachungsrelevante Dienstmerkmale müssen die notwendigen Informationen in den nationalen Parametern übermittelt werden. Die Inhalte der Parameter müssen mit der Bundesnetzagentur abgestimmt werden.	
5.4.4 5.5.2, 5.5.3, 5.5.11	**Multi party calls – general principles** Bei CW, HOLD und MPTY (bis sechs Teilnehmer) kann alternativ Option A oder Option B genutzt werden. Bei mehr als sechs Teilnehmern in einer großen Konferenz muss Option B realisiert werden.	Für CW, HOLD, MPTY bis sechs Teilnehmer gilt: Da die Mehrfachnutzung der ISDN-Kanäle zur berechtigten Stelle nach Option B eine komplexere Zuordnung sowie eine erschwerte Auswertung der Nutzinformationen (keine Sprecherdifferenzierung per Kanal) bedingt, soll bevorzugt Option A implementiert werden.
5.4.5	**Subscriber Controlled Input** Bei Registrierungs- und Aktivierungsvorgängen sind Ereignisdaten auch dann zu erzeugen, wenn die Steuerung von Betriebsmöglichkeiten auf indirektem Weg (z.B. über eine Servicenummer oder per Webzugriff) geschieht.	Diese Forderung richtet sich nach § 5 Abs. 1 Nr. 4 TKÜV. Die jeweiligen Ereignisse und zugehörigen Daten sind mit der Bundesnetzagentur im Einzelfall abzustimmen.
5.5.3	**Call Hold/Retrieve** Bei Aktivierung von HOLD müssen beide CC links während der HOLD-Phase stumm geschaltet werden. Darüber hinaus wird die Option akzeptiert, bei der nur die gehaltene Kennung (held party) stumm geschaltet wird.	
5.5.4	**Explicit Call Transfer (ECT)** Nach dem Transfer muss die Option 2 realisiert werden (“The transferred call shall not be intercepted.”).	
5.5.15	**User-to-User Signalling (UUS)** Die Nutzinformationen des Dienstes UUS werden als Ereignisdaten übermittelt.	Siehe Abschnitt 5.3.1 und 5.4 dieser Tabelle.
Chapter 6: Packet data domain		

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
6.4	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜV.	siehe Ergänzung 2 dieser Tabelle.
6.5.0	**PacketDirection** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzdaten mit *to target* bzw. *from target* zu erfolgen. **IP-Adressen und Port-Nummern** Zur Übermittlung der Quell- und Ziel-IP-Adressen sowie der zugehörigen Portnummern der Kommunikationsteilnehmer sind die Parameter *sourceIPAddress*, *destinationIPAddress, sourcePortNumber* und *destinationPortNumber* zu verwenden.	
6.5.1.1	**REPORT record information** The REPORT record shall be triggered when as a national option, a mobile terminal is authorized for service with another network operator or service provider.	Diese Option ist in Deutschland nicht zu realisieren. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
6.6	**IRI reporting for packet domain at GGSN** As a national option, in the case where the GGSN is reporting IRI for an intercept subject, the intercept subject is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to report the following IRI of the content of communication: - PDP context activation; - PDP context deactivation; - Start of interception with PDP context active.	Diese Option muss in Deutschland nicht realisiert werden. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
6.7	**Content of communication interception for packet domain at GGSN** As a national option, in the case where the GGSN is performing interception of the content of communications, the intercept subject is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to perform the interception of the content of communication.	Diese Option darf in Deutschland nur dann realisiert werden, wenn die Forderung gemäß § 4 Abs. 1 TKÜV erfüllt ist. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
Chapter 7: Multimedia domain		

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
7.1.2	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
7.2.1	**Timing** Alle Zeitstempel sind generell als local time auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*. siehe Anlage A.4 der TR TKÜV.
7.3	**Security aspects**. Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Anlage A2 der TR TKÜV vorgesehen.
7.4	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜV	
7.5	**IRI for IMS** Im Parameter 'SIPmessage' müssen im Falle einer IRIonly-Überwachung die Nutzinhalte wie bspw. SMS-Inhalte oder sonstige Messaging-Inhalte (z.B. Immediate Messaging) vor der Ausleitung entfernt werden.	
7.5.1	**Events and information** Die Parameter Correlation number und Correlation nach Tabelle 2 müssen berichtet werden. Der Parameter mediaDecryption-info. CCKeyInfo.cCSalt muss berichtet werden, sofern dem Verpflichteten dieser Wert vorliegt.	Wird Verschlüsselung netzseitig eingesetzt, muss diese am Übergabepunkt aufgehoben werden (§ 8 Abs. 3 TKÜV). Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente bzw. die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der bS übermitteln. Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
Chapter 8: 3GPP WLAN Interworking		

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
		Soweit in Deutschland öffentlich zugängliche Dienste gemäß Abschnitt 8 der Spezifikation 3GPP TS 33.108 angeboten werden, sind grundsätzlich die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Dienste sind mit der Bundesnetzagentur abzustimmen.
Chapter 9: Interception of Multimedia Broadcast/MultiCast Service (MBMS)		
		Soweit in Deutschland öffentlich zugängliche Dienste gemäß Abschnitt 9 der Spezifikation 3GPP TS 33.108 angeboten werden, sind grundsätzlich die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Dienste sind mit der Bundesnetzagentur abzustimmen.
Chapter 10: Evolved Packet System (EPS)		
10.1.2	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
10.2.1	**Timing** Alle Zeitstempel sind generell auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*. siehe Anlage A.4 der TR TKÜV.
10.3	**Security aspects**. Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Anlage A2 der TR TKÜV vorgesehen.
10.4	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜV	
10.5.0	**PacketDirection** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzdaten mit *to target* bzw. *from target* zu erfolgen. **IP-Adressen und Port-Nummern** Zur Übermittlung der Quell- und Ziel-IP-Adressen sowie der zugehörigen Portnummern der Kommunikationsteilnehmer sind die Parameter *sourceIPAddress*, *destinationIPAddress, sourcePortNumber* und *destinationPortNumber* zu verwenden.	

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
10.5.1.1.5	**Tracking Area Update (REPORT) old location information** Provide (only by the old MME), when authorized and if available, to identify the old location information for the intercept subject's MS.	Dieser Parameter muss berichtet werden, sofern dieser Wert für die Überwachungsfunktionalität des Verpflichteten verfügbar ist.
10.5.1.4.1	**Bearer Deactivation (END) EPS bearer id**	Dieser Parameter muss berichtet werden, sofern dieser Wert für die Überwachungsfunktionalität des Verpflichteten verfügbar ist.
10.6	**IRI reporting for evolved packet domain at PDN-GW** Unter bestimmten Bedingungen (bspw. Roaming) kann das PDN-GW die einzige Möglichkeit zur Überwachung darstellen. In diesen Fällen muss die Überwachungsfunktionalität für die Erfassung und Ausleitung vor Ereignisdaten (IRIs) gemäß Abschnitt 10.6 der 3GPP-Spezifikation 33.108 am PDN-GW realisiert werden.	Diese Option muss in Deutschland nicht realisiert werden. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
10.7	**CC interception for evolved packet domain at PDN-GW** Unter bestimmten Bedingungen (bspw. Roaming) kann das PDN-GW die einzige Möglichkeit zur Überwachung darstellen. In diesen Fällen muss die Überwachungsfunktionalität für die Erfassung und Ausleitung vor Nutzinhalten (CC) gemäß Abschnitt 10.7 der 3GPP-Spezifikation 33.108 am PDN-GW realisiert werden.	Diese Option darf in Deutschland nur dann realisiert werden, wenn die Forderung nach § 4 Abs. 1 der TKÜV erfüllt ist. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
Chapter 11: 3GPP IMS Conference Services		
		Soweit in Deutschland öffentlich zugängliche Dienste gemäß Abschnitt 11 der Spezifikation 3GPP TS 33.108 angeboten werden, sind grundsätzlich die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Dienste sind mit der Bundesnetzagentur abzustimmen.

Annex A: HI2 delivery mechanisms and procedures

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
A.1.2.3.1	**Data link establishment** Optionally a *Data link test* procedure may be used to verify periodically the data link.	Diese Option ist aufgrund der Entscheidung, FTP als Übertragungsprotokoll für die IRI zu nutzen, nicht relevant.
A.2	**FTP** Zur Übermittlung der IRI muss in Deutschland FTP eingesetzt werden. Es muss die 'File naming method B' genutzt werden. Zusätzlich gelten die Bestimmungen der Anlage A.1 und A.2 der TR TKÜV.	
Annex C: UMTS HI3 interface		
C	**UMTS HI3 Interface** Die alternative Nutzung des ULIC-Headers Version 0 oder Version 1 bzw. FTP ist den Verpflichteten freigestellt.	Auf Seiten der bSn müssen alle Optionen (ULIC Version 0 und Version 1 sowie FTP) unterstützt werden.
C.1.1	**Introduction** In Deutschland ist die Übermittlungsmethode TCP/IP vorgesehen.	Für die Übermittlung ~~werden~~ wird auf Seiten der bS (destination port number) die Portnummer ~~50000~~ 50010 festgelegt. ~~Alternativ kann auch Port 50010 verwendet werden.~~
C.1	**UMTS LI correlation header** In Deutschland muss die Option ULICv1 implementiert werden. Bei Nutzung des ULIC-header version 1 sind die Parameter LIID und timeStamp zu verwenden (mandatory).	
Annex J: Use of sub-address and calling party number to carry correlation information		
J.2.3.2	**Field order and layout** Die Parameter für die Zuordnung von CC und IRI nach Table J.2.3 und J.2.4 sind entsprechend zu verwenden. Zudem ist in den Oktetts 17-23 der Called Party Subaddress (Table E.3.4 und E.3.6) als Unterscheidungskriterium zu den Subadressen nach den Festlegungen der Anlage B der TR TKÜV das feste Bitmuster '45 54 53 49 20 56 32' hex = ETSI V2' einzutragen.	Nach den rein nationalen Festlegungen für leitungsvermittelnde Netze (Anlage B der TR TKÜV) werden ebenfalls Subadressen genutzt, jedoch mit einer anderen Besetzung. Damit die Auswerteeinrichtung der bS eine Unterscheidung treffen kann, muss dieses Unterscheidungsmerkmal zwingend erfolgen.

Anlage D.2 Erläuterungen zu den ASN.1-Beschreibungen

Die Bundesnetzagentur informiert gemäß § 11 Satz 5 TKÜV auf ihrer Internetseite über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage D sind aus den verschiedenen Versionen der 3GPP -Spezifikation TS 33.108 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung von FTP als Übertragungsprotokoll sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in der Spezifikation als 'conditional’ und 'optional’ bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in der Spezifikation bzw. nach Anlage D.1 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, z.B. ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder z.B. DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

Die Übermittlung administrativer Ereignisse (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme sowie Fehlermeldungen) sowie zusätzlicher Ereignisse (z.B. bezüglich herstellereigener Dienste) erfolgt nach Anlage A.3.

Anlage E Übergabepunkt für Speichereinrichtungen für Sprache, Faksimile und Daten (Voicemail-Systeme, Unified-Messaging-Systeme etc.)

Diese Anlage beschreibt die nationalen Anforderungen an den Übergabepunkt für Speichereinrichtungen (UMS, VMS etc.). Da in den Festlegungen nach den Anlagen B bis D derartige Systeme nicht berücksichtigt sind, müssen diese Anforderungen ggf. zusätzlich erfüllt werden.

Neben den Anforderungen nach Teil A, Abschnitte 3 und 4, sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Kopie der Nutzinformation erfolgt nach dieser Anlage E zusammen mit den Ereignisdaten in einer XML-kodierten Datei, die per FTAM/X.25 oder FTP/Internet übertragen werden kann. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten.
Anlage A.2	Teilnahme am VPN mittels Kryptobox Wird die Übermittlung der Überwachungskopie per FTP/Internet vorgenommen, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage E.1 Begriffsbestimmungen

Unified-Messaging-System (UMS) Alle Varianten von in Telekommunikationsnetzen betriebenen Speichereinrichtungen, die i.d.R. für mehrere Telekommunikationsarten vorgesehen sind, wie Sprache, Fax, E-Mail, Short Messages, Multimedia Messaging Service (MMS) usw.

(UMS)Box Der Teil des Unified-Messaging-Systems, der einem bestimmten Teilnehmer, in den hier zu betrachtenden Fällen dem züA, zugeordnet ist.

Anlage E.2 Allgemeine Erläuterungen

Bei der technischen Umsetzung angeordneter Maßnahmen zur Überwachung der Telekommunikation ist im Zusammenhang mit UMS die systembedingte Besonderheit zu beachten, dass hier keine Echtzeitkommunikation zwischen dem züA und seinem jeweiligen Partner besteht. Diese Besonderheit hat Auswirkungen auf einige Aspekte der technischen Umsetzung derartiger Überwachungsmaßnahmen, insbesondere hinsichtlich der Übermittlung der zu Überwachungskopie an die bS:

- die Aufteilung der zu überwachenden Telekommunikation in eine Sende- und eine Empfangsrichtung und deren getrennte Übermittlung ist nicht erforderlich,
- infolge der in diesen Fällen nicht gegebenen Echtzeitanforderungen können neue sinnvolle und zugleich wirtschaftliche Möglichkeiten der Übermittlung der zu überwachenden Telekommunikation in Betracht gezogen werden.

Die Kopie der Nutzinformationen aus den vorgenannten Speichereinrichtungen kann mit einem geringfügigen Zeitversatz an die bS übermittelt werden, dabei hat diese Übermittlung jedoch so zeitnah wie möglich zu erfolgen: beim Einstellen der Nachricht in die Speichereinrichtung spätestens im unmittelbaren Anschluss an den Speichervorgang, beim Abruf der Nachricht mit einem Zeitversatz von nicht mehr als 10 Sekunden.

Wenn die vollständige Kopie einer bestimmten Nachricht bereits übermittelt worden ist, genügt es bei weiteren Ereignissen (z. B. beim nachfolgenden Abhören der Nachricht) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der bS zugeordnet werden können, muss ein eindeutiges Zuordnungsmerkmal in dem Feld Zuordnungsnummer vorgesehen werden.

Da eine Überwachungsanordnung nur die während des darin festgelegten Zeitraums in die UMS eingestellte, abgerufene bzw. kopierte Telekommunikation erfasst, dürfen Nachrichten, die bereits vor diesem Zeitraum in der UMS gespeichert waren, nicht überwacht werden. Diese wären erst dann zu erfassen, wenn diese beispielsweise abgerufen werden.

Anlage E.3 Grundsätzliche Ausleitungsmethoden sowie Festlegung von relevanten Ereignissen

Anlage E.3.1 Grundsätzliche Ausleitungsmethoden der zu überwachenden Telekommunikation

Die in Unified-Messaging-Systemen gespeicherten Telekommunikationsarten Sprache, Fax und SMS können grundsätzlich in Verbindung einer Implementierung nach den Anlagen B, C, D oder H überwacht bzw. ausgeleitet werden. Alternativ besteht die Möglichkeit, diese Telekommunikationsarten in einer XML-kodierten Datei per FTP oder FTAM an die bS zu übertragen.

In UMS gespeicherte Multimediamessages (MMS) werden ebenfalls in einer XML-kodierten Datei per FTP oder FTAM an die bS übertragen. Zudem können MMS grundsätzlich mit dem in Anlage H beschriebenen Übergabepunkt zur bS übertragen werden.

Sieht die UMS darüber hinaus Funktionen des Dienstes E-Mail vor bzw. wird der E-Mail Dienst zur Übermittlung der Nachrichten genutzt, ist der Übergabepunkt für diese Telekommunikationsart nach Anlage E zu gestalten. Darüber hinaus ist grundsätzlich freigestellt, für sämtliche Telekommunikationsarten die Ausleitung nach Anlage E vorzunehmen, z.B. dann, wenn diese in Form von E-Mail in der UMS gespeichert werden.

Die nachfolgende Tabelle stellt die einzelnen Möglichkeiten nochmals dar:

Content	**Ausleitungsmethoden**
Sprache	mittels einer ISDN 64 kbit/s Verbindung mit dem ISDN-Bearer-Service 'Unrestricted Digital Information (UDI)' nach Anlage B, C oder D.
	mittels RTP-Verbindungen nach Anlage H (die dabei genutzte Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).
	im wav- oder mp3-Format innerhalb einer XML-kodierten Datei [2)] zusammen mit den Ereignisdaten nach Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
Fax	mittels einer ISDN 64 kbit/s Verbindung mit Unterstützung der Prozeduren nach ITU-T Empfehlung T.30 und dem ISDN-Teleservice 'Facsimile Gr. 2/3'nach Anlage B, C oder D.
	mittels RTP-Verbindungen nach Anlage H (die dabei genutzte Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).
	im tif-, jpg- oder png-Format innerhalb einer XML-kodierten Datei [1)] zusammen mit den Ereignisdaten nach Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
SMS [3)]	in einem Ereignisdatensatz nach Anlage B, C oder D.
	mittels RTP-Verbindungen oder SIP-Messages nach Anlage H (die dabei genutzte Methode sowie die Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).
	als SMS innerhalb einer XML-kodierten Datei [1)] zusammen mit den Ereignisdaten nach Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
Multimedia-messages (MMS)	im E-Mail Format innerhalb einer XML-kodierten Datei [1)] zusammen mit den Ereignisdaten nach Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
	mittels RTP-Verbindungen oder SIP-Messages nach Anlage H (die dabei genutzte Methode sowie die Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).

E-Mail	in einer XML-kodierten Datei zusammen mit den Ereignisdaten mittels FTP nach Anlage F.

Tabelle Anlage E.3.1-1 Ausleitungsmethoden bei UMS

[1)] Bei der Kodierung sind ausschließlich offene Kodierungsverfahren zu verwenden.

[2)] Zur Übermittlung der XML-kodierten Datei an die bS gelten die bezüglich der Übermittlung und der Schutzanforderungen gemachten Anforderungen zu den Ereignisdaten nach Anlage B, C, D und H

Kann beim ersten Verbindungsversuch die Datei mit der Kopie der Nutzinformation sowie den Ereignisdaten nicht zu der bS übermittelt werden, sind in einem Zeitintervall von wenigen Minuten drei weitere Übermittlungsversuche durchzuführen. Weitere Einzelheiten sind in der Anlage A.4 enthalten.

[3)] Der Nachrichtentext einer SMS oder einer MMS ist der bS als Text mit Zeichensatz nach UTF-8 zu übermitteln. Zur Übermittlung des Nachrichteninhaltes einer SMS kann alternativ der Inhalt der kompletten PDU (inkl. SM Header, User data header, User data) entsprechend der Spezifikation 3GPP TS 23.040 in hexadezimaler Form angegeben werden. Dies entspricht der Anforderung nach Anlage B, C, D bzw. H.

Anlage E.3.2 Grundsätzliche Festlegung von relevanten Ereignissen

Bei den folgenden grundsätzlichen Ereignissen ist eine Ausleitung der Kopie der Nutzinformation sowie der Ereignisdaten vorzusehen. Verfügt die UMS über Dienstmerkmale, die durch diese Ereignisse nicht erfasst werden (z.B. Rückanruf als Reaktion einer hinterlegten Sprachnachricht), so sind die diesbezüglichen Anforderungen mit der Bundesnetzagentur abzustimmen:

Ereignis	Bemerkungen
Aufsprechen bzw. Einstellen	Aufsprechen bzw. Einstellen einer Nachricht (Sprache, Fax oder SMS) in das UMS mittels: • Anrufweiterschaltung über die Kennung des züA oder • Einwählen bzw. Versenden von einem beliebigen Anschluss (z.B. direktes Einwählen in das UMS über eine Servicerufnummer order per Webzugang)
Abfragen bzw. Auslesen	Abfragen bzw. Auslesen einer Nachricht (Sprache, Fax oder SMS) aus dem UMS über: • die Kennung des züA bzw. durch Anwahl dieser Kennung mit anschließender Anrufweiterschaltung zum UMS • einen beliebigen Anschluss (z.B. direktes Einwählen in das UMS über eine Servicerufnummer order per Webzugang)
Kopieren von Speicherinhalten	Kopieren von Speicherinhalten von einer der Kennung des züA zugeordneten Box in eine andere Box und umgekehrt
Zugriff auf die Box und Modifikation von Einstellungen	Die möglichen Ereignisse (z.B. Einstellen einer Benachrichtigungsnummer, Erstellen von Versandlisten) müssen individuell mit der Bundesnetzagentur abgestimmt werden.

Tabelle Anlage E.3.2-1 Ereignisse in UMS

Anlage E.4 Anforderungen für die Überwachung von Sprach- und Faxnachrichten sowie von SMS nach Anlagen B, C oder D

Die nachfolgenden abweichenden Anforderungen bzw. Präzisierungen gelten bei Ausleitung von Sprach- und Faxnachrichten mittels ISDN-Verbindungen sowie SMS mittels eines Ereignisdatensatzes nach den Prinzipien der Anlage B, C oder D für leitungsvermittelnde Netze.

lfd. Nr.	Abweichende Anforderungen bzw. Präzisierungen	Bemerkungen
A. Ausleitung der Kopie von Sprachnachrichten		
1	Die an die bS zu übermittelnde Information besteht aus der kompletten Sprachnachricht einschließlich eines vorhandenen Begrüßungstextes (Ansage) und einem vorhandenen Ende-Kennzeichen (z.B. Ton oder Textansage).	Ein jeweils identischer Begrüßungstext bzw. ein jeweils identischer Ende-Kennzeichen kann alternativ einmalig beim Beginn der Überwachungsmaßnahme übermittelt werden. Bei einer etwaigen Änderung muss der Inhalt neu an die bS übermittelt werden.
2	Die Übermittlung erfolgt mittels einer ISDN 64 kbit/s Verbindung mit dem ISDN-Bearer-Service 'Unrestricted Digital Information (UDI)'. Der Verbindungsaufbau durch das UMS erfolgt automatisch, wobei die Kopie der Sprachnachricht zuvor in eine der bS zugeordnete Box kopiert werden kann. Die Zuordnungskriterien werden nach den Anforderungen der Anlage B, C oder D in der Subadresse übermittelt.	Zur Übermittlung reicht eine ISDN-Stich aus (mono mode), d. h. ein Doppelstich für Sende- und Empfangsrichtung wie bei der Überwachung eines Telefonanschlusses ist hier nicht erforderlich. Falls die Übermittlung an die bS nicht möglich ist, erfolgen drei weitere Verbindungsversuche im Abstand von wenigen Minuten, z.B. 3 Minuten (siehe auch Anlage A.4).
3	Es sind die in den Anlagen B, C oder D vorgesehenen Schutzanforderungen (CLI, CUG) einzuhalten. Eine von der bS gesendete 'Connected Number' darf nicht überprüft werden.	Dies ist nötig, damit seitens der bS zum Empfang von Faxnachrichten auf andere Kennungen umgeleitet werden kann.
4	Der Inhalt sowie die Übermittlung von Ereignisdatensätzen richten sich nach dem Teil D dieser Tabelle	

B. Ausleitung der Kopie von Faxnachrichten		
1	Die an die bS zu übermittelnde Kopie der Faxnachricht besteht aus der kompletten Faxnachricht, wie sie der züA bzw. dessen Kommunikationspartner erhält.	
2	Die Übermittlung erfolgt mit Unterstützung der Prozeduren nach ITU-T Empfehlung T.30 und dem ISDN-Teleservice 'Facsimile Gr. 2/3', d. h. Bearer Capability BC = 'audio 3,1 kHz' und High Layer Compatibility HLC = 'Facsimile Gr 2/3'. Der Verbindungsaufbau durch das UMS erfolgt automatisch, wobei die Kopie der Sprachnachricht zuvor in eine der bS zugeordnete Box kopiert werden kann. Die Zuordnungskriterien werden nach den Anforderungen der Anlage B, C oder D in der Subadresse übermittelt. Zusätzlich wird die Referenznummer (bei Anlage B alternativ die Rufnummer des züA) sowie die Zuordnungsnummer im Header der Faxnachricht an die bS übermittelt	Zur Übermittlung reicht eine ISDN-Stich aus (mono mode), d. h. ein Doppelstich für Sende- und Empfangsrichtung wie bei der Überwachung eines Telefonanschlusses ist hier nicht erforderlich. Die Aufzeichnungseinrichtungen der bSn unterstützen dabei die Prozeduren nach ITU-T Empfehlung T.30 Falls die Übermittlung an die bS nicht möglich ist, erfolgen drei weitere Verbindungsversuche im Abstand von wenigen Minuten, z.B. 3 Minuten (siehe auch Anlage A.4). Durch die Übermittlung der Zuordnungskriterien sowohl in der Subadresse als auch im Header können seitens der bS sowohl integrierte Einrichtungen mit der Möglichkeit der automatischen Subadressen-Auswertung als auch handelsübliche Fax-Geräte mit manueller Zuordnung eingesetzt werden.

lfd. Nr.	Abweichende Anforderungen bzw. Präzisierungen	Bemerkungen
3	Es sind die in den Anlagen B, C oder D vorgesehenen Schutzanforderungen (CLI, CUG) einzuhalten. Eine von der bS gesendete 'Connected Number' darf nicht überprüft werden.	Dies ist nötig, damit seitens der bS zum Empfang von Faxnachrichten auf andere Kennungen umgeleitet werden kann.
4	Der Inhalt sowie die Übermittlung von Ereignisdatensätzen richten sich nach dem Teil D dieser Tabelle	
C. Ausleitung der Kopie von SMS-Nachrichten		
1	Die an die bS zu übermittelnde Kopie der SMS-Nachricht besteht aus dem Nachrichteninhalt in UTF-8 oder der kompletten PDU (inkl. SM Header, User data header, User data).	
2	Die Übermittlung erfolgt in einem Ereignisdatensatz. Der Verbindungsaufbau durch das UMS erfolgt automatisch, wobei die Kopie der SMS-Nachricht zuvor in eine der bS zugeordnete Box kopiert werden kann.	In den entsprechenden Anlagen sind jeweils Parameter vorgesehen. Falls die Übermittlung an die bS nicht möglich ist, erfolgen drei weitere Verbindungsversuche im Abstand von wenigen Minuten, z.B. 3 Minuten (siehe auch Anlage A.4).
3	Es sind die in den Anlagen B, C oder D vorgesehenen Schutzanforderungen (CUG bzw. VPN) zur Übermittlung von Ereignisdaten einzuhalten.	
4	Der Inhalt sowie die Übermittlung von sonstigen Ereignisdatensätzen richten sich nach dem Teil D dieser Tabelle	
D. Inhalt und Übermittlung der begleitenden Ereignisdaten		
1	Bei jedem in der Tabelle Anlage E-1.1 genannten Ereignis wird ein Ereignisdatensatz erzeugt und nach den Vorgaben der Anlage B, C oder D übermittelt. Das zu berichtende Ereignis wird bei einer Implementierung nach Anlage B im Feld 13 ('Dienstmerkmal') und bei einer Implementierung nach den Anlagen C oder D im national Parameter berichtet.	Mögliche Ereignisse sind: • Aufsprechen einer Sprachnachricht • Anhören einer Sprachnachricht • Zugriff auf die Box • Empfang einer Box-to-Box Nachricht • Benachrichtigungen über vorhandene Nachrichten per SMS oder E-Mail • Änderung der Benachrichtigungsnummer • Erstellen oder Ändern von Versandlisten

Tabelle Anlage E.1.3-2 Abweichende Anforderungen bzw. Präzisierungen bei UMS

Anlage E.5 Anforderungen für die Überwachung von Sprach- und Faxnachrichten, SMS sowie MMS innerhalb einer XML-kodierten Datei

Alternativ zu der Ausleitung nach Anlage E.4 können die Kopien der verschiedenen Telekommunikationsarten Sprache, Fax, SMS und MMS einheitlich über eine XML-kodierte Datei mittel FTP oder FTAM übertragen werden.

Die verschiedenen Telekommunikationsarten sind dabei in ein Dateiformat entsprechend der nachfolgenden Tabelle umzuwandeln. Die Tabelle wird mit der Einführung neuer Technologien erweitert. Dazu sind eventuell neu zu definierende Parameter mit der Bundesnetzagentur abzustimmen.

Parameter (Tag)	**Anwendung**
<audio-wav>	Sprachnachricht im wav-Format
<audio-mp3>	Sprachnachricht im mp3-Format
<fax-tif>	Faxnachricht im TIFF-Format
<fax-jpg>	Faxnachricht im JPEG-Format
<fax-png >	Faxnachricht im PNG- Format
<sms>	Short Message
<mms>	Multimedia Message Die zu überwachende MMS wird in der Weise als E-Mail dargestellt, dass der Nachrichtentext im Textfeld und die zugehörige Bilder als Anlage beigefügt werden. Im E-Mail-Header werden keine Parameter eingetragen.

Tabelle Anlage E.5-1 Parameter (Tag) der Dateiformate

Anlage E.5.1Parameter der Ereignisdaten

Die einzelnen Parameter der Ereignisdaten, die i.d.R. zusammen mit der Kopie der Nutzinformationen in einer XML-kodierten Datei zusammengefasst an die bS übertragen wird, sind in der nachfolgenden Tabelle aufgelistet:

Parameter	**Werte/Definition/Erläuterung**
<Versionskennung>	Kennung, die vom Betreiber der TKA-V vergeben wird und die jeweilige Version der Schnittstelle bezeichnet im ASCII-Format (max. 20 Zeichen)
<Datensatzart>	'report' als Kennung für ein einmaliges Ereignis
<Referenznummer>	Kennzeichnungsmerkmal der Überwachungsmaßnahme gemäß § 7 Abs. 2 Satz 1 TKÜV im ASCII-Format
<Zuordnungsnummer>	Zuordnung zu den Nutzinformationen im ASCII-Format (Werte von 1 bis 65535)
<Kennung-des-züA>	Merkmal der zu überwachenden Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 1 TKÜV (z.B. dem UMS zugeordnete Telefondienst- oder Fax-Rufnummer nach E.164, E-Mail-Adresse)
<Partner-Kennung> [1)]	Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV von der eine Nachricht eingestellt oder abgerufen wird bzw. Einstellungen vorgenommen werden (z.B. Rufnummer des Anschlusses, dem das UMS zugeordnet ist, Servicerufnummer)
<IP> [1)]	Die zum UMS übermittelte IP-Adresse gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV (die IP-Adresse des Telekommunikationspartners, z.B. beim Abrufen oder Einstellen von Nachrichten über Webzugang, wenn keine Rufnummer als Partner-Kennung vorhanden ist)
<Beginn>	Beginn der zu überwachenden Telekommunikation (z.B. Zeitpunkt des Einstellens einer Nachricht) gemäß § 7 Abs. 1 Satz 1 Nr. 8 TKÜV im Format: TT/MM/JJ hh:mm:ss Die Datei mit den Ereignisdaten und/oder Nutzinformationen ist erst nach Abschluss des zu überwachenden Telekommunikationsvorgangs zu den bS zu übermitteln.

Parameter	Werte/Definition/Erläuterung
<Einstellungen>	1. Nähere Angaben zu den vorgenommenen Einstellungen des UMS, beginnend mit dem Ereignis: '**zugriff**' (des Box-Inhabers auf die Box), '**erstellen-von-Versandlisten**', '**messaging**' (Einstellungen im Benachrichtungsdienst), '**Ansagetext**', '**aenderung**' (sonstige Box-Einstellungen), 2. und anschließender Angabe der durchgeführten Einstellungen (Parameter) im Format: freier ASCII-kodierter Text Die beiden Angaben sind durch ';' (ASCII-Zeichen Nr. 59) zu trennen.
<Richtung>	Nähere Angabe über das zu berichtende Ereignis, z.B.: 'empfangen', 'abgerufen', 'anhoeren' (von Nachrichten), 'empfang-box-to-box', 'eingestellt', 'gesendet', 'aufsprechen' (von Nachrichten), 'versenden-box-to-box', 'benachrichtigung' (über vorhandene Nachrichten)*, 'callback'*[2)]*.* Sind mehrere Ereignisse quasi zeitgleich, z.B. eingestellt und versendet, können auch zwei Werte, getrennt durch ';' (ASCII-Zeichen Nr. 59), eingetragen werden.
<Ausloesegrund-zueA>	Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde, z.B.: • 'erfolgreich' oder • Fehlermeldung des Systems als Textstring, z.B. Abbruch bei einem Download. Für den Textstring sind nur ASCII-Zeichen des Base64-Alphabets erlaubt.
<Beginn-UEM>	Einmalig je Maßnahme mit dem Zeitpunkt der Aktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss
<Ende-UEM>	Einmalig je Maßnahme mit dem Zeitpunkt der Deaktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss

Tabelle E.5.1-1: Parameter der Ereignisdaten der XML-Datei

[1)] Dadurch soll erreicht werden, dass wenn keine eindeutige <Partner-Kennung> verfügbar ist, zumindest die IP-Adresse übermittelt werden muss.

[2)] Ist es dem Box-Inhaber des VMS/UMS möglich, aufgrund einer empfangenen Nachricht einen Anruf zu dem Anschluss zu initiieren, von dem die Nachricht eingestellt wurde, muss einerseits dieses neue Ereignis berichtet werden und andererseits sichergestellt sein, dass auch der Anruf überwacht wird. Eine Korrelation des Ereignisses 'callback' mit der hinterlegten Nachricht mit dem Parameter <Zuordnungsnummer> ist nicht nötig.

Anlage E.5.2 Die XML-Struktur und DTD für Sprache, Fax, SMS und MMS

Die XML-kodierte Datei muss im UTF-8-Format erzeugt werden. In einer Datei können optional auch mehrere Überwachungskopien in paketierter Weise übertragen werden

In dem nachfolgenden Beispiel einer XML-Struktur sind für alle Tags Werte eingetragen. Diese sind jedoch nur entsprechend dem jeweiligen Ereignis zu übermitteln. Wenn zu den jeweiligen Ereignisdaten keine Parameter vorhanden sind, ist entsprechend der XML-Syntax ein leeres Tag zu verwenden, beispielsweise "<Beginn-UEM/>". Die Kommentarzeilen werden nicht benötigt und können weggelassen werden.

XML Structure für die nicht-paketierte Übermittlung (mit Beispieleinträgen):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-ums SYSTEM "hi3-ums_v1.dtd">
<?xml-stylesheet href="ums_v1.xsl" type="text/xsl"?>
<hi3-ums>
<Versionskennung>ABC1234</Versionskennung>
```

```
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[123 in Base64-Kodierung [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64-Kodierung
[1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64-Kodierung
[1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[Ansagetext;freier Text in Base64-Kodierung
[1]]]></Einstellungen>
<Richtung><!CDATA[abgerufen in Base64-Kodierung [1]]]></Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64-Kodierung
[1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden SMS in Base64-Kodierung [1]]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden MMS wird hier im E-Mail-Format in
Base64-Kodierung [1]eingefügt]]>
<!-- Ende MMS -->
</mms>

</hi3-ums>
```

Doctype Definition:

<!ELEMENT hi3-ums (Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer,Kennung-des-zueA,IP,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-UEM,Ende-UEM,fax-tif,fax-jpg,fax-png,audio-wav,audio-mp3,sms,mms)>
<!ELEMENT Versionskennung (#PCDATA)>
<!ELEMENT Datensatzart (#PCDATA)>
<!ELEMENT Referenznummer (#PCDATA)>
<!ELEMENT Zuordnungsnummer (#PCDATA)>
<!ELEMENT Kennung-des-zueA (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT Partner-Kennung (#PCDATA)>
<!ELEMENT Beginn (#PCDATA)>
<!ELEMENT Einstellungen (#PCDATA)>
<!ELEMENT Richtung (#PCDATA)>
<!ELEMENT Ausloesegrund-zueA (#PCDATA)>
<!ELEMENT Beginn-UEM (#PCDATA)>
<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT fax-tif (#PCDATA)>
<!ELEMENT fax-jpg (#PCDATA)>
<!ELEMENT fax-png (#PCDATA)>
<!ELEMENT audio-wav (#PCDATA)>
<!ELEMENT audio-mp3 (#PCDATA)>
<!ELEMENT sms (#PCDATA)>
<!ELEMENT mms (#PCDATA)>

[1] Die Werte der einzelnen Tags bzw. die Kopie der zu überwachenden Nachricht muss base64-kodiert nach RFC 822 bzw. RFC 2045 [26] eingebunden werden. Bitte beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

XML Structure für die paketierte Übermittlung (Beispiel mit zwei Einzelereignissen):

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-ums-pack SYSTEM "hi3-ums_pack_v1.dtd">
<?xml-stylesheet href="ums_p.xsl" type="text/xsl"?>

<hi3-ums-pack>
<hi3-ums id[2]=“1“>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[123 in Base64-Kodierung [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64-Kodierung [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64-Kodierung [1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[Ansagetext;freier Text in Base64-Kodierung [1]]]></Einstellungen>
<Richtung><![CDATA[abgerufen in Base64-Kodierung [1]]]></Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64-Kodierung [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden SMS in Base64-Kodierung [1]]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden MMS wird hier im E-Mail-Format in Base64-Kodierung [1]eingefügt]]>
<!-- Ende MMS -->
</mms>
</hi3-ums>

<hi3-ums id[2]="2">
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[124 in Base64-Kodierung [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64-Kodierung [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64-Kodierung [1]]]></Partner-Kennung>
<Beginn>14/02/07 10:10:05</Beginn>
<Einstellungen><![CDATA[Ansagetext;freier Text in Base64-Kodierung [1]]]></Einstellungen>
<Richtung>><![CDATA[abgerufen in Base64-Kodierung[1]]]</Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64-Kodierung [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/02/07 01:00:00</Beginn-UEM>
<Ende-UEM>01/03/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-tif -->

```
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden SMS in Base64-Kodierung [1]]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden MMS wird hier im E-Mail-Format in
Base64-Kodierung [1]eingefügt]]>
<!-- Ende MMS -->
</mms>
</hi3-ums>

</hi3-ums-pack>
```

Doctype Definition (für die paketierte Übermittlung):

```
<!ELEMENT hi3-ums-pack (hi3-
ums,Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer,Kennung-des-
zueA,IP,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-
UEM,Ende-UEM,fax-tif,fax-jpg,fax-png,audio-wav,audio-mp3,sms,mms)>
<ATTLIST hi3-ums
id CDATA   #REQUIRED>
<!ELEMENT Versionskennung (#PCDATA)>
<!ELEMENT Datensatzart (#PCDATA)>
<!ELEMENT Referenznummer (#PCDATA)>
<!ELEMENT Zuordnungsnummer (#PCDATA)>
<!ELEMENT Kennung-des-zueA (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT Partner-Kennung (#PCDATA)>
<!ELEMENT Beginn (#PCDATA)>
<!ELEMENT Einstellungen (#PCDATA)>
<!ELEMENT Richtung (#PCDATA)>
<!ELEMENT Ausloesegrund-zueA (#PCDATA)>
<!ELEMENT Beginn-UEM (#PCDATA)>
```

<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT fax-tif (#PCDATA)>
<!ELEMENT fax-jpg (#PCDATA)>
<!ELEMENT fax-png (#PCDATA)>
<!ELEMENT audio-wav (#PCDATA)>
<!ELEMENT audio-mp3 (#PCDATA)>
<!ELEMENT sms (#PCDATA)>
<!ELEMENT mms (#PCDATA)>

[1] Die Werte der einzelnen Tags bzw. die Kopie der zu überwachenden Nachricht muss base64-kodiert nach RFC 822 bzw. RFC 2045 [26] eingebunden werden. Bitte beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

[2] Das Attribut „id“ ist zwecks Differenzierbarkeit der Datensätze mit unterschiedlichen Werten zu belegen.

Anlage F Festlegungen für Speichereinrichtungen des Dienstes E-Mail

Diese Anlage enthält zwei alternative Beschreibungen des Übergabepunktes zur Überwachung des Dienstes E-Mail:

- Anlage F.2 definiert einen nationalen Übergabepunkt, bei dem die Kopie der E-Mail zusammen mit den Ereignisdaten in einer XML-Datei per FTP zur bS übermittelt wird.
- Die alternative Beschreibung des Übergabepunktes nach Anlage F.3 richtet sich nach der ETSI-Spezifikation TS 102 233 bzw. TS 102 232-02 [30] und beschreibt eine ASN.1-Datei, die ebenfalls die gesamte Überwachungskopie enthält und TCP/IP zur Übermittelung nutzt.

Neben den Anforderungen nach Teil A, Abschnitte 3 und 4, sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Wird die Übermittlung der Kopie der E-Mail erfolgt nach dieser Anlage F.2 zusammen mit den Ereignisdaten in einer XML-kodierten Datei per FTP/Internet übertragen wird, gelten die Festlegungen in Anlage A.1 enthalten.
Anlage A.2	Teilnahme am VPN mittels Kryptobox. Wird die Übermittlung der Überwachungskopie per FTP/Internet nach Anlage F.2 vorgenommen, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage F.1 Begriffsbestimmungen, Grundsätzliches

E-Mail-Server Alle Varianten von Telekommunikationsanlagen, die Nachrichten des Dienstes E-Mail speichern oder übermitteln, unabhängig von den Zugangsmöglichkeiten des Nutzers, z.B. SMTP, POP3, IMAP, WEB oder WAP.

E-Mail-Adresse Adresse nach RFC 822, RFC 2822.
Die E-Mail-Adresse ist eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

E-Mail-Postfach Speicherplatz für E-Mail-Nachrichten eines Nutzers (E-Mail-Account), in dem gesendete sowie ankommende Nachrichten aufbewahrt werden. Ein zu überwachendes E-Mail-Postfach kann u.U. ein Postfach für mehrere E-Mail-Adressen sein.

Login Vorgang, bei der die Zugangsberechtigung eines Teilnehmers oder

sonstigen Endnutzers zu seinem E-Mail-Postfach geprüft wird.

Login-Name Der beim Login als Teil der Zugangskennung verwendete Login-Name ist neben der E-Mail-Adresse ebenfalls eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

In einer Anordnung zur Überwachung der Telekommunikation beim Dienst E-Mail kann als technisches Merkmal genannt werden:

- eine E-Mail-Adresse oder
- die Zugangskennung (Login-Name ohne Passwort) eines E-Mail-Postfachs.

Um die Überwachung der vollständigen Telekommunikation, die unter der Kennung abgewickelt wird, durchzuführen, muss besonders bei ausgehendem Verkehr (z.B. Versenden von E-Mails mittels SMTP) sichergestellt werden, dass die überwachte Telekommunikation tatsächlich dem züA durch die Verwendung von geeigneten Authentifizierungsmethoden zuzuordnen ist. Dadurch soll beispielsweise verhindert werden, dass eine zu überwachende E-Mail bei der Versendung nur deswegen nicht erfasst wird, weil die Absenderadresse durch den Nutzer manipuliert wurde.

Während bei der Überwachung auf der Grundlage eines Login-Namens diese Anforderung durch die Authentifizierungsprozedur des Login (Login-Name und Passwort) i.d.R. erfüllt ist, kann eine Überwachung aufgrund einer E-Mail-Adresse nur dann umgesetzt werden, wenn die eingesetzten, protokollbezogen Authentifikationsmethoden diese Anforderung erfüllen. Die Anlage F.2 enthält Erläuterungen zu den hierzu zulässigen Authentifikationsmethoden.

Kann diese Anforderung (z.B. wegen einer ungeeigneten Authentifikationsmethode) für eines der Protokolle SMTP, POP3 oder IMAP nicht erfüllt werden, muss ersatzweise für dieses Protokoll eine auf die E-Mail-Adresse bezogene Anordnung durch die Überwachung des gesamten E-Mail-Postfachs durchgeführt werden, bei der die Telekommunikation aller E-Mail-Adressen dieses Postfachs erfasst werden muss. Wenn für den Zugang zum E-Mail-Postfach ebenfalls keine systemintegrierte Authentifizierungsprozedur vorgesehen ist, muss mit der Bundesnetzagentur eine andere Authentifizierungsprozedur bzw. ein anderes Verfahren abgestimmt werden, die bzw. das es ermöglicht, dennoch ausschließlich die Telekommunikation des züA zu überwachen.

Die Nutzinformation, die aus der vollständigen Kopie der zu überwachenden E-Mail (Header, Body und Attachment) besteht, und die dazugehörigen Ereignisdaten werden in einer Datei zusammengefügt. Diese Datei ist per FTP zur bS unmittelbar nach dem jeweiligen Ereignis zu übermitteln. In einer Datei können optional auch mehrere Überwachungskopien in paketierter Weise übertragen werden.

In Fällen, in denen lediglich die Überwachung der Ereignisdaten angeordnet ist, sind nur diese (ohne Nutzinformationen) zur bS zu übermitteln.

Anlage F.2 National spezifizierter E-Mail-Übergabepunkt

Wenn die vollständige Kopie einer bestimmten E-Mail bereits an die bS übermittelt worden ist, genügt es, bei weiteren Ereignissen nach den Tabellen F.2-1-1 bis F.2-1-4 (z. B. beim nachfolgenden Abrufen der E-Mail) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der bS zugeordnet werden können, muss ein eindeutiges Zuordnungsmerkmal in dem Feld Zuordnungsnummer vorgesehen werden.

Die Auflistung nach den Tabellen F.2-1-1 bis F.2-1-4 muss abhängig von den jeweiligen Möglichkeiten des konkreten E-Mail-Servers entsprechend ergänzt bzw. verändert werden.

Bei den folgenden Ereignissen ist grundsätzlich eine Ausleitung der Nutzinformation sowie der Ereignisdaten an die bS vorzusehen:

Simple Mail Transfer Protocol (SMTP)

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweise zur Belegung des XML-Parameters <Partner-Kennung>
Empfangen einer E-Mail	Unabhängig davon, ob diese dem zu überwachenden Nutzer direkt zugestellt oder in dem E-Mail-Postfach gespeichert werden.	'empfangen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender (Envelope: MAIL FROM gem. RFC 2822), jedoch nicht die weiteren Empfänger (Envelope: RCPT TO gem. RFC 2822), anzugeben. Die Kennung des züA ist in einem RCPT TO-Feld des Envelopes oder im TO-Feld des Headers der E-Mail enthalten.
Einstellen einer E-Mail [1)]	Eine E-Mail wird vom zu überwachenden Nutzer an den Mail-Server übertragen.	'eingestellt'	Bei den von der zu überwachenden E-Mail-Adresse ausgehenden E-Mails ist im Ereignisdatenfeld <Partner-Kennung> der Inhalt aller Adressfelder , mit Ausnahme des ZÜA (ENVELOPE: RCPT TO gem. RFC 2822) einzutragen
Versenden einer E-Mail	Der E-Mail-Server versendet eine eingestellte E-Mail.	'gesendet'	
Weiterleiten einer E-Mail	E-Mails, welche empfangen und anschließend weitergeleitet werden.	'gesendet'	

Tabelle F.2-1-1 Ereignisse 'SMTP'

[1)] Das Ereignis 'Einstellen einer E-Mail' ist ebenfalls für eingestellte bzw. geänderte Entwürfe einer E-Mail, unabhängig vom hierfür genutzten Protokoll, vorgesehen, auch wenn diese zunächst beispielsweise ohne E-Mail-Adressen und ohne Betreffzeile eingestellt werden.

Zulässige Methoden der Authentifikation:

- Der SMTP-Server fordert beim Verbindungsaufbau prinzipiell eine explizite Authentifikation per SMTP-AUTH an.
- Der Teilnehmer meldet sich zunächst über den Posteingangs-Server bei seinem E-Mail-Postfach an und authentifiziert sich dabei mit seinen Zugangsdaten (Benutzername und Passwort). Anschließend verbleibt ihm ein beschränktes Zeitfenster zum Versenden von E-Mails per SMTP. („SMTP after POP“). Die Anforderung nach Anlage F.1.2 an die Authentifikation ist nur bei entsprechend geringem Zeitfenster erfüllt.
- Der Teilnehmer erhält eine IP-Adresse, welche als Kriterium für die Authentifikation verwendet wird.
- Wenn der E-Mail-Anbieter zugleich auch der Zugangsanbieter ist, ist es zulässig, wenn die bei der Netzeinwahl stattgefundene Authentifikation für den E-Mail-Dienst übernommen wird.

Für das Ereignis „Empfangen einer E-Mail“ ist die Authentifikation nicht relevant, da bei überwachter Telekommunikation eingehende E-Mails grundsätzlich ausgeleitet werden müssen.

Post Office Protocol Version 3 (POP3)

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweise zur Belegung des XML-Parameters <Partner-Kennung>
Abrufen einer E-Mail	Der zu überwachende Nutzer ruft eine E-Mail aus seinem E-Mail-Postfach ab, vollständig oder teilweise (z.B. nur den Header, 'Betreff' oder Anhang).	'abgerufen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender, jedoch nicht die weiteren Empfänger einzutragen. Der anzugebende Wert ergibt sich aus dem MAIL-BODY.

Tabelle F.2-1-2 Ereignisse 'POP3'

Zulässige Methoden der Authentifikation:

- Der Teilnehmer meldet sich bei seinem E-Mail-Postfach an, per Login auf der Webseite[1] bzw. auf dem POP3-Server und authentifiziert sich dabei mit seinen Zugangsdaten (Login-Name und Passwort), bevor E-Mails abgerufen werden können.

Internet Message Access Protocol (IMAP)

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweise zur Belegung des XML-Parameters <Partner-Kennung>
Einstellen einer E-Mail [2)]	Eine vom E-Mail-Client erzeugte Nachricht wird in einem IMAP-Verzeichnis abgelegt (mittels IMAP-Kommando APPEND) und anschließend mit dem Server abgeglichen.	'eingestellt'	Bei diesen E-Mails ist im Ereignisdatenfeld <Partner-Kennung> der Inhalt aller Adressfelder, mit Ausnahme des züA einzutragen. Der anzugebende Wert ergibt sich aus dem MAIL-BODY.
Abrufen einer E-Mail	Der zu überwachende Nutzer ruft eine E-Mail aus seinem E-Mail-Postfach ab; vollständig oder teilweise (z.B. nur den Header, 'Betreff' oder Anhang). Bei IMAP sind jedoch nur die E-Mails zu überwachen, die zwischen Client und Server aufgrund einer Synchronisation der Ordner (als neue E-Mail) übertragen werden.	'abgerufen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender, jedoch nicht die weiteren Empfänger einzutragen. Der anzugebende Wert ergibt sich aus dem MAIL-BODY.

Tabelle F.2-1-3 Ereignisse 'IMAP'

2) Das Ereignis 'Einstellen einer E-Mail' ist ebenfalls für eingestellte bzw. geänderte Entwürfe einer E-Mail, unabhängig vom hierfür genutzten Protokoll, vorgesehen, auch wenn diese zunächst beispielsweise ohne E-Mail-Adressen und ohne Betreffzeile eingestellt werden.

Zulässige Methoden der Authentifikation:

- Der Teilnehmer meldet sich bei seinem E-Mail-Postfach an, per Login auf der Webseite[1] bzw. auf dem IMAP-Server und authentifiziert sich dabei mit seinen Zugangsdaten (Login-Name und Passwort), bevor E-Mails abgerufen, eingestellt oder verschoben werden können.

[1] gilt für Webmail-Dienste, welche auf IMAP bzw. POP3 basieren.

Broadcast-Nachricht

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweis
Versenden einer E-Mail als Broad-cast-Nachricht	Der E-Mail-Server leitet eine vom zu überwachenden Nutzer empfangene E-Mail weiter.	'zugestellt'	Bei einem Broadcast-Senden wird auf die Sicherstellung der Empfangsbereitschaft des Clients sowie dessen Empfangsquittierung verzichtet. (z.B. SkyDSL).

Tabelle F.2-1-4 Ereignisse beim Versenden einer Broadcast-Nachricht

Anmerkungen zu den o.g. Tabellen:

- Die mehrfache Übermittlung inhaltsgleicher Datensätze zwischen verschiedenen physikalischen Teilen eines logischen IMAP-Servers zur berechtigten Stelle ist nur zulässig, sofern dies auf Fetch- oder Append-Kommandos zur Synchronisation der Server- oder Client-Verzeichnisse zurückzuführen ist.
- E-Mail, die vom SMTP-Server empfangen und anschließend unmittelbar an die vom Nutzer des
  E-Mail-Postfachs voreingestellte E-Mail-Adresse weitergeleitet werden, sind grundsätzlich auch zu überwachen. Im Parameter <Richtung> ist beim Empfangen der Wert 'empfangen' und beim anschließenden Versenden der Wert 'gesendet' zu verwenden.
- Die Kopie jeder zu überwachenden E-Mail muss mit den dazugehörigen Ereignisdaten ereignisbezogen entsprechend der in Anlage F.2.1 aufgeführten Tabelle F.2-1 in jeweils einer XML-kodierten Datei zusammengefasst werden. Dabei ist die vollständige Kopie der E-Mail, d.h. Adressfelder, Betreff, Haupttext und evt. Anhänge, nach Base64 zu kodieren. Nach der Base64-Kodierung muss nach jeweils 76 Zeichen einen Zeilenumbruch enthalten.
- Die XML-kodierte Datei wird per FTP zur bS übermittelt. Bezüglich der Gestaltung des Dateinamens, der FTP-Parameter, des Sicherung durch ein VPN sowie zum Verfahren bei Übermittlungshindernissen siehe Anlage A1 bis A4.

Anlage F.2.1Parameter der Ereignisdaten

Die einzelnen Parameter der Ereignisdaten, die i.d.R. zusammen mit der Kopie der Nutzinformationen in einer XML-kodierten Datei zusammengefasst an die bS übertragen wird, sind in der nachfolgenden Tabelle aufgelistet:

Parameter	Definition/Erläuterung
<Versionskennung>	Kennung, die vom Betreiber der TKA-V vergeben wird und die jeweilige Version der Schnittstelle bezeichnet
<Datensatzart>	'Report' als Kennung für ein einmaliges Ereignis
<Referenznummer>	Kennzeichnungsmerkmal der Überwachungsmaßnahme gemäß § 7 Abs. 2 Satz 1 TKÜV im ASCII-Format (1 bis 25 Stellen, Zeichenvorrat 'a'...'z', 'A'...'Z', '-', '_', '.', und '0'...'9'). Der nutzbare Zeichenvorrat entspricht den Implementierungen nach ETSI/3GPP.
<Zuordnungsnummer>	Zuordnung zu den Nutzinformationen Hierbei muss die Message-ID (nach RFC 2822) der zu überwachenden E-Mail verwendet werden. Diese kann als Kopie dem E-Mail-Header oder den Envelope-Daten entnommen werden.
<Kennung des züA>	Merkmal der überwachenden Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 1 TKÜV (z.B. E-Mail-Adresse oder Benutzerkennung des E-Mail-Postfachs)

Parameter	Definition/Erläuterung
<Partner-Kennung>[1]	Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV Die Belegung des Parameters ist abhängig vom jeweiligen Protokoll (s. Tabelle F.2-1-1 bis F.2-1-3). Mehrere Partner-Kennungen sind getrennt durch ';' (ASCII-Zeichen Nr.59) anzugeben.
<IP>	Die aus Sicht des E-Mail-Servers bekannte IP-Adresse des E-Mail-Clients, von dem aus E-Mail eingestellt oder abgerufen bzw. Einstellungen vorgenommen werden.
<Port>	Kennung für das verwendete Übertragungsprotokoll (z.B. HTTP, SMTP, POP3). Bei Implementierungen auf der Grundlage der Ausgabe 4.1 der TR TKÜV dürfen die Portnummern (z.B. 80, 25, 110) nur dann weiterhin genutzt werden, wenn diese Angaben nach den entsprechenden well known ports erfolgen.
<Beginn>	Beginn der zu überwachenden Telekommunikation (z.B. Zeitpunkt des Empfangs einer E-Mail) gemäß § 7 Abs. 1 Satz 1 Nr. 8 TKÜV im Format: TT/MM/JJ hh:mm:ss Die Datei mit den Ereignisdaten und/oder Nutzinformationen ist erst nach Abschluss des zu überwachenden Telekommunikationsvorgangs zu den bSn zu übermitteln.
<Einstellungen>	Beinhaltet zwei Angaben, die durch ';' (ASCII-Zeichen Nr. 59) zu trennen sind: 1. Nähere Angaben zu den folgenden vorgenommenen Einstellungen: '**zugriff**' (Erfolgreicher Login des Postfach-Inhabers), **versandlisten** (inkl. von Änderungen)', '**messaging**' (z.B. Einstellungen im Benachrichtigungsdienst), '**weiterleitung**' (z.B. Einstellungen zur Weiterleitung von E-Mail), **email-adresse**' (z. B. Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im zu überwachenden Postfach), 2. und anschließender Angabe der durchgeführten Einstellungen (Parameter) im Format: freier, ASCII-kodierter Text.
<Richtung>	Nähere Angabe über das zu berichtende Ereignis nach den Tabellen F.2-1-1 bis -4: 'empfangen', 'abgerufen', 'gesendet', 'eingestellt', 'zugestellt'. Sind mehrere Ereignisse quasi zeitgleich, z.B. eingestellt und versendet, können auch zwei Werte, getrennt durch ';' (ASCII-Zeichen Nr. 59), eingetragen werden.
<Ausloesegrund-zueA>	Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde, z.B.: • 'erfolgreich' oder • Fehlermeldung des Systems als Textstring, z.B. Abbruch bei einem Download. Für den Textstring sind nur ASCII-Zeichen in der Base64-Codierung erlaubt.
<Beginn-UEM>	Einmalig je Maßnahme, enthält den Zeitpunkt der Aktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss
<Ende-UEM>	Einmalig je Maßnahme, enthält den Zeitpunkt der Deaktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss

Tabelle F.2.1: Parameter der Ereignisdaten der XML-Datei

[1] Die empfangende bS muss bei der Auswertung berücksichtigen, dass veränderte Partner-Kennungen grundsätzlich nicht erkannt werden können (z.B. 'AlCapone@Alcatraz.com' statt der tatsächlichen Email-Adresse).

Anlage F.2.2XML-Struktur und DTD

Die XML-kodierte Datei muss im UTF-8 Format erzeugt werden.

In dem nachfolgenden Beispiel einer XML-Struktur sind für alle Tags Werte eingetragen. Diese sind jedoch nur entsprechend dem jeweiligen Ereignis zu übermitteln. Wenn zu den jeweiligen Ereignisdaten keine Parameter vorhanden sind, ist entsprechend der XML-Syntax ein leeres Tag zu verwenden, beispielsweise "<Beginn-UEM/>". Kommentarzeilen werden nicht benötigt und können weggelassen werden.

XML-Struktur (Beispiel für die nicht-paketierte Übermittlung):

<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<!DOCTYPE hi3-email SYSTEM "hi3-email_v1.dtd">

<?xml-stylesheet href="E-Mail_v1.xsl" type="text/xsl"?>

<hi3-email>

<Versionskennung>ABC1234</Versionskennung>

<Datensatzart>report</Datensatzart>

<Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>

<Zuordnungsnummer><![CDATA[0474745765656 in Base64-Kodierung [1]]]></Zuordnungsnummer>

<Kennung-des-zueA><![CDATA[ueberwach.Adresse@zueA.de in Base64-Kodierung [1]]]></Kennung-des-zueA>

<IP>111.222.63.254</IP>

<Port>SMTP</Port>

<Partner-Kennung><![CDATA[Adresse1@domain1.de; Adresse2@domain2.de in Base64-Kodierung [1]]]></Partner-Kennung>

<Beginn>31/12/06 10:10:05</Beginn>

<Einstellungen><![CDATA[weiterleitung; freier Text in Base64-Kodierung [1]]]></Einstellungen>

<Richtung><![CDATA[abgerufen in Base64-Kodierung [1]]]></Richtung>

<Ausloesegrund-zueA><![CDATA[erfolgreich in Base64-Kodierung [1]]]></Ausloesegrund-zueA>

<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>

<Ende-UEM>01/02/07 01:00:00</Ende-UEM>

<email>

<!-- Beginn E-Mail -->

<![CDATA[Die Kopie der zu ueberwachenden E-Mail in Base64-Kodierung [1]]]>

<!-- Ende E-Mail -->

</email>

</hi3-email>

Doctype Definition (für die nicht-paketierte Übermittlung):

<!ELEMENT hi3-email (Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer,Kennung-des-zueA,IP,Port,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-UEM,Ende-UEM,email)>

<!ELEMENT Versionskennung (#PCDATA)>

<!ELEMENT Datensatzart (#PCDATA)>

<!ELEMENT Referenznummer (#PCDATA)>

<!ELEMENT Zuordnungsnummer (#PCDATA)>

<!ELEMENT Kennung-des-zueA (#PCDATA)>

<!ELEMENT IP (#PCDATA)>

<!ELEMENT Port (#PCDATA)>

<!ELEMENT Partner-Kennung (#PCDATA)>

<!ELEMENT Beginn (#PCDATA)>

<!ELEMENT Einstellungen (#PCDATA)>
<!ELEMENT Richtung (#PCDATA)>
<!ELEMENT Ausloesegrund-zueA (#PCDATA)>
<!ELEMENT Beginn-UEM (#PCDATA)>
<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT email (#PCDATA)>

[1] Die Werte der einzelnen Tags bzw. die Kopie der zu überwachenden E-Mail muss base64-kodiert nach RFC 822 bzw. RFC 2045 eingebunden werden. Es ist dabei zu beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

XML-Struktur (Beispiel für die paketierte Übermittlung von zwei Einzelereignissen):

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-email-pack SYSTEM "hi3-email_pack_v1.dtd">
<?xml-stylesheet href="E-Mail_p_v1.xsl" type="text/xsl"?>
<hi3-email-pack>
<hi3-email id[2]=“1“>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[0474745765656 in Base64-Kodierung [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[ueberwach.Adresse@zueA.de in Base64-Kodierung [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Port>SMTP</Port>
<Partner-Kennung><![CDATA[Adresse1@domain1.de; Adresse2@domain2.de in Base64-Kodierung [1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[weiterleitung; freier Text in Base64-Kodierung [1]]]></Einstellungen>
<Richtung><![CDATA[abgerufen in Base64-Kodierung [1]]]></Richtung>
<Ausloesegrund-zueA><![CDATA[erfolgreich in Base64-Kodierung [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>
<email>
<!-- Beginn E-Mail -->
<![CDATA[Die Kopie der zu ueberwachenden E-Mail in Base64-Kodierung [1]]]>
<!-- Ende E-Mail -->
</email>

</hi3-email>
<hi3-email id[2]=“2“>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[0474745765657 in Base64-Kodierung [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[ueberwach.Adresse@zueA.de in Base64-Kodierung [1]]]></Kennung-des-zueA>

<IP>111.222.63.254</IP>

<Port>IMAP</Port>

<Partner-Kennung><![CDATA[Adresse1@domain1.de; Adresse2@domain2.de in Base64-Kodierung [1]]]></Partner-Kennung>

<Beginn>01/01/07 10:10:05</Beginn>

<Einstellungen><![CDATA[versandlisten; freier Text in Base64-Kodierung [1]]]></Einstellungen>

<Richtung><![CDATA[abgerufen in Base64-Kodierung [1]]]></Richtung>

<Ausloesegrund-zueA><![CDATA[erfolgreich in Base64-Kodierung [1]]]></Ausloesegrund-zueA>

<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>

<Ende-UEM>01/02/07 01:00:00</Ende-UEM>

<email>

<!-- Beginn E-Mail -->

<![CDATA[Die Kopie der zu ueberwachenden E-Mail in Base64-Kodierung [1]]]>

<!-- Ende E-Mail -->

</email>

</hi3-email>

</hi3-email-pack>

Doctype Definition (für die paketierte Übermittlung):

<!ELEMENT hi3-email-pack (hi3-email,Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer, Kennung-des-zueA,IP,Port,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-UEM,Ende-UEM,email)>

<ATTLIST hi3-email

id CDATA #REQUIRED>

<!ELEMENT Versionskennung (#PCDATA)>

<!ELEMENT Datensatzart (#PCDATA)>

<!ELEMENT Referenznummer (#PCDATA)>

<!ELEMENT Zuordnungsnummer (#PCDATA)>

<!ELEMENT Kennung-des-zueA (#PCDATA)>

<!ELEMENT IP (#PCDATA)>

<!ELEMENT Port (#PCDATA)>

<!ELEMENT Partner-Kennung (#PCDATA)>

<!ELEMENT Beginn (#PCDATA)>

<!ELEMENT Einstellungen (#PCDATA)>

<!ELEMENT Richtung (#PCDATA)>

<!ELEMENT Ausloesegrund-zueA (#PCDATA)>

<!ELEMENT Beginn-UEM (#PCDATA)>

<!ELEMENT Ende-UEM (#PCDATA)>

<!ELEMENT email (#PCDATA)>

[1] Die Werte der einzelnen Tags bzw. die Kopie der zu überwachenden E-Mail muss base64-kodiert nach RFC 822 bzw. RFC 2045 eingebunden werden. Es ist dabei zu beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

[2] Das Attribut „id“ ist zwecks Differenzierbarkeit der Datensätze mit unterschiedlichen Werten zu belegen.

Anlage F.3 E-Mail-Übergabepunkt nach ETSI TS 102 232-02 (ab Version 2.1.1)

Als Alternative zu dem national spezifizierten Übergabepunkt nach Anlage F.2 besteht auch die Möglichkeit, den Übergabepunkt nach ETSI TS 102 232-02 [30] zu gestalten.

Hierzu gelten die Grundsätze nach Anlage F.1.

Wenn die vollständige Kopie einer bestimmten E-Mail bereits an die bS übermittelt worden ist, genügt es, bei weiteren Ereignissen (E-Mail-Events) nach Abschnitt 6, ETSI TS 102 232-02 (z. B. beim nachfolgenden Abrufen der E-Mail) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der bS zugeordnet werden können, muss ein eindeutiges Zuordnungsmerkmal vorgesehen werden.

Neben den in TS 102 232-02 definierten Events sind Einstellungen bezüglich der E-Mail-Adresse bzw. des E-Mail-Postfachs zu berichten, wenn diese in den Zeitraum der Anordnung fallen. Hierzu sind Eintragungen im ASN.1-Feld *National-EM-ASN1parameters* des ASN.1-Moduls nach TS 102 232-02 vorzunehmen. In Anlage A.3 ist hierzu das nationale ASN.1-Modul definiert (siehe Anforderung zum Berichten von Einstellungen nach Anlage F.3.1.2).

Abhängig vom zu erfassenden Ereignis ist der ASN.1-Parameter `E-Mail Recipient List` entsprechend zu belegen (siehe Anforderung nach Anlage F.3.1.2).

Anlage F.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage F.3.1.1 Grundlage: ETSI TS 102 232-01

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-01 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1-Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als *delivery country code* 'DE' zu verwenden. Der *operator identifier* wird nach Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der *network element identifier* ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die *communication identity number* kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Abs. 2 Satz 2 TKÜV vorgesehenen Zuordnungsnummer.

Abschnitt TS 102 232-01	**Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam vermeiden und die Reihenfolge sicherstellen.
5.2.6	**Payload timestamp** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) als~~:~~ ~~*GeneralizedTime* sowie im Format des~~ *MicroSecondTimeStamp* (mit höchster Auflösung und Genauigkeit) anzugeben. ~~anzugeben.~~ Der *MicroSecondTimeStamp* muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	Mit der TR TKÜV, Ausgabe 7.0 ist nur noch der *Micro-SecondTimeStamp* zu verwenden. Ist der Zeitstempel nicht im Format des *MicroSecondTimeStamp* am Interceptionpoint verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.~~Die Kodierung des Parameters *GeneralizedTime* erfolgt als universal time und ohne time difference.~~ ~~Die zusätzliche Zeitangabe als *MicroSecondTimeStamp* soll insbesondere in Fehlerfällen die Rekonstruktion der Teillieferungen ermöglichen.~~
5.2.11	**Interception Point Identifier** Der interception point identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.~~;~~	
6.2.2	**Error Reporting** Die Übermittlung richtet sich grundsätzlich nach Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist grundsätzlich vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem maßnahmenbezogenen Einsatz von Padding muss die jeweilige bS zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt grundsätzlich Abschnitt ~~5.1~~3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der bS zu verhindern.	

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
6.3.4	**Keep-alives** Kann optional vom Verpflichteten implementiert werden.	Grundsätzlich muss die TCP-Verbindung nach erfolgreicher Übermittlung von Daten timer-gesteuert abgebaut werden. Dem maßnahmenbezogenen Einsatz von Padding Keep-alives, bei der die TCP-Verbindung ständig aufrecht erhalten bleibt, muss die jeweilige bS zustimmen.
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der bS (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 und TS 102 232-06.
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements** Es gelten die Anforderungen nach Anlage A.2 der TR TKÜV.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden.
7.3.2	**Timeliness** Eine eventuelle Nutzung separater *managed networks* ist zwischen dem Verpflichteten und den bSn abzustimmen.	

Anlage F.3.1.2 Grundlage: ETSI TS 102 232-02

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-02 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-02	**Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
6.2.3, 6.3.3, 6.4.3	**IRI informations** Die in den Tabellen 1, 2 und 3 dargestellten IRI-Informationen für die Events „E-Mail send“, „E-Mail receive“ und „E-Mail download“ müssen grundsätzlich übermittelt werden.	Siehe hierzu auch Punkt “E-mail format“
7	**E-mail attributes** Die E-Mail-Attribute sind entsprechend der Vorgaben der Spezifikation zu übermitteln. Dies gilt insbesondere für das Attribut „AAAInformation“. Darüber hinaus sind die nebenstehenden Anforderungen zu beachten.	**7.3 E-mail recipient list** Bei E-Mails, welche für die zu überwachende Kennung bestimmt sind, ist lediglich der Sender, jedoch nicht die weiteren Empfänger, wie bspw. CC- und/oder BCC-Empfänger anzugeben. **7.10 AAAInformation** Parameter einer POP3- bzw. SMTP-Authentifikation, wie etwa „username“, „password“, „authMethod“ etc. sind ebenfalls zu berichten.
A.4, B.4, C.2	**HI2 event-record mapping** Neben den beschriebenen Events müssen die Einstellungen zu folgenden Dienstmerkmalen berichtet werden: - **Versandlisten** (inkl. Änderungen), - **Messaging** (z.B. Einstellungen zu einem Benachrichtigungsdienst) - **Weiterleitung** (autom. Weiterleitung von E-Mails) Bei der Überwachung eines E-Mail-Postfachs zusätzlich: - **E-Mail-Adresse** (z.B. Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im Postfach)	Zur Übermittlung von Einstellungen wird das nationale ASN.1-Modul nach Anlage A.3.2 dieser TR TKÜV verwendet, welches mittels ASN.1-Modul der TS 102 232-02 zur berechtigten Stelle übermittelt wird.
Annex D	**E-mail format** Bei der Nutzung von well-known ports und der Implementierung des E-Mail Formats "ip-packet" müssen die Parameter der IRI-Informationen „client address“, „server-Address“ sowie „client port“ und „server-Port“ nicht zusätzlich berichtet werden, da diese den jeweiligen IP- bzw. TCP-Header-Daten entnommen werden können.	Bei IRI-Only Maßnahmen müssen diese dennoch besetzt werden.

Anlage F.3.2Erläuterungen zu den ASN.1-Beschreibungen

Die Bundesnetzagentur informiert gemäß § 11 Satz 5 TKÜV auf ihrer Internetseite über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage F.3 sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-01 sowie TS 102 232-02 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung von FTP als Übertragungsprotokoll sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in den Spezifikationen als 'conditional’ und 'optional’ bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach Anlage F.3 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, z.B. ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder z.B. DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153' H)

Die Übermittlung administrativer Ereignisse (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme sowie Fehlermeldungen) sowie zusätzlicher Ereignisse (z.B. bezüglich herstellereigener Dienste) erfolgt nach Anlage A.3.

Anlage G Festlegungen für den Internetzugangsweg (ETSI TS 102 232-03, -04 sowie TS 101 909-20-2)

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt nach den ETSI-Spezifikationen TS 102 232-03 [31], TS 102 232-04 [32] und TS 101 909-20-2 [33] für diejenigen Übertragungswege (z.B. xDSL, CATV, WLAN), die dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dienen.
Diese ETSI-Spezifikationen nutzen jeweils den generellen IP-basierten Übergabepunkt, wie er in der
ETSI-Spezifikationen TS 102 232-01 [29] beschrieben ist.

Die Anlage beinhaltet die Entscheidung über die in den Spezifikationen enthaltenen Optionen und die Festlegungen ergänzender technischer Anforderungen.

Werden neben dem Internetzugangsdienst auch Rundfunkverteildienste oder ähnliche für die Öffentlichkeit bestimmte Dienste (z.B. IP-TV, Video on demand) mittels vom Betreiber des Internetzugangsweges betriebenen Plattformen bzw. Einspeisepunkten über diesen Internetzugangsweg realisiert, für die nach § 3 Abs. 2 Nr. 4 TKÜV keine Vorkehrungen getroffen werden müssen, sollen diese Telekommunikationsanteile möglichst nicht in der Überwachungskopie des Internetzugangs enthalten sein.

Werden hingegen individualisierte Verteildienste angeboten, die nicht für die Öffentlichkeit angeboten werden (z.B. Verteilen selbst erstellter Inhalte an geschlossene Nutzergruppen) fallen diese Telekommunikationsanteile nicht unter die Entpflichtung des § 3 Abs. 2 Nr. 4 TKÜV und müssen bei der Überwachung miterfasst werden.

Neben den Anforderungen nach Teil A, Abschnitte 3 und 4, sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.2	Teilnahme am VPN mittels Kryptobox. Da die Übermittlung der Überwachungskopie per TCP/IP über das Internet erfolgt, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage G.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage G.1.1 Grundlage: ETSI TS 102 232-01

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-01 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-01	**Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1 Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als *delivery country code* 'DE' zu verwenden. Der *operator identifier* wird nach Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der *network element identifier* ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die *communication identity number* kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Abs. 2 Satz 2 TKÜV vorgesehenen Zuordnungsnummer.
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam vermeiden und die Reihenfolge sicherstellen.
5.2.6	**Payload timestamp** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) als~~:~~ ~~*GeneralizedTime* sowie im Format des~~ *MicroSecondTimeStamp* (mit höchster Auflösung und Genauigkeit) anzugeben. ~~anzugeben.~~ Der *MicroSecondTimeStamp* muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	Mit der TR TKÜV, Ausgabe 7.0 ist nur noch der *Micro-SecondTimeStamp* zu verwenden. Ist der Zeitstempel nicht im Format des *MicroSecondTimeStamp* am Interceptionpoint verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren. ~~.Die Kodierung des Parameters *GeneralizedTime* erfolgt als universal time und ohne time difference.~~ ~~Die zusätzliche Zeitangabe als *MicroSecondTimeStamp* soll insbesondere in Fehlerfällen die Rekonstruktion der Teillieferungen ermöglichen.~~

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.7	**Payload direction** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzdaten mit *to target* bzw. *from target* zu erfolgen.	
6.2.2	**Error Reporting** Die Übermittlung richtet sich grundsätzlich nach Anlage A.4 der TR TKÜV.	
5.2.11	**Interception Point Identifier** Der interception point identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.~~,~~	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist grundsätzlich vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem maßnahmenbezogenen Einsatz von Padding muss die jeweilige bS zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt grundsätzlich Abschnitt ~~5.1~~3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der bS zu verhindern.	
6.3.4	**Keep-alives** Für die verpflichtende Verwendung von *Keep-Alives* sind die Vorgaben der grundsätzlichen Anforderungen aus Teil A, Punkt 3.3 zu beachten.	Grundsätzlich muss die TCP-Verbindung nach erfolgreicher Übermittlung von Daten timer-gesteuert abgebaut werden. Dem maßnahmenbezogenen Einsatz von Keep-alives, bei der die TCP-Verbindung ständig aufrechterhalten bleibt, muss die jeweilige bS zustimmen.
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der bS (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 und TS 102 232-06..
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements** Es gelten die Anforderungen nach Anlage A.2 der TR TKÜV.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden.
7.3.2	**Timeliness** Eine eventuelle Nutzung separater *managed networks* ist zwischen dem Verpflichteten und den bSn abzustimmen.	

Anlage G.1.2 Grundlage: ETSI TS 102 232-03

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-03 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-03	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.3.1	**Target Identity** Grundsätzlich gelten die Forderungen nach Abschnitt 6 der TR TKÜV. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis einer Kabelmodemkennung möglich, doch muss berücksichtigt werden, dass an den zu überwachenden Internetzugangsweg ein anderes Kabelmodem angeschaltet werden kann oder das "überwachte" Kabelmodem an einen anderen Internetzugangsweg angeschaltet werden kann.
4.3.2	**Result of interception** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) anzugeben.	Die Kodierung des Parameters GeneralizedTime erfolgt als universal time und ohne time difference.
6.1	**Events** Es sind die Events und HI2 Attribute ab Version 1.4.1 der ETSI-Spezifikation zu verwenden.	Mit der Version 1.4.1 wurde der Event 'startOfInterceptionWithSessionActive' ergänzt.
8	**ASN.1 for IRI and CC** Für diese Fälle nach § 7 Abs. 3 TKÜV muss die enthaltene ASN.1 Beschreibung für "IRIOnly" nicht implementiert werden.	Für diese Fälle müssen neben den administrativen Daten (z.B. LIID) lediglich die ASN.1 Daten des '**IPIRIContents**' übermittelt werden. Dies entspricht der Regelung, dass bei solchen Anordnungen lediglich der CC-Anteil nicht zu übermitteln ist.

Anlage G.1.3 Grundlage: ETSI TS 102 232-04

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-04 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-04	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.2.1	**Target Identity** Grundsätzlich gelten die Forderungen nach Abschnitt 6 der TR TKÜV. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis der MAC Adresse eines Modems möglich, doch muss berücksichtigt werden, dass an den zu überwachenden Internetzugangsweg ein anderes Modem angeschaltet werden kann oder das "überwachte" Modem an einen anderen Internetzugangsweg angeschaltet werden kann.

Abschnitt TS 102 232-04	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.3.2	**Result of interception** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) anzugeben.	Die Kodierung des Parameters GeneralizedTime erfolgt als universal time und ohne time difference.
6.1	**Events** Es sind die Events und HI2 Attribute nach Version 1.3.1 der ETSI-Spezifikation zu verwenden.	Mit der Version 1.3.1 wurde der Event 'End of Interception Session_Active ' gelöscht.
8.2	**ASN.1 specification** Für die Fälle nach § 7 Abs. 3 TKÜV kann die enthaltene ASN.1 Beschreibung für "IRIOnly" anstatt der Beschreibung der ASN.1 Daten ' **L2IRIContents**' implementiert werden.	In diesen Fällen ist lediglich der Auf- und Abbau eines Layer2-Tunnels bekannt.

Anlage G.1.4 Grundlage ETSI TS 101 909-20-2

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 101 909-20-2 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 101 909-20-2	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.2	**Architecture** Es wird eine Implementierung auf der Grundlage des EuroDOCSIS vorausgesetzt.	Abhängig von der Gestaltung der TKA-V, insbesondere des Diensteumfangs kann die Bundesnetzagentur eine bestimmte Version des Standards vorgeben.
5	**LI architecture for IP multimedia Time Critical Services** Die Spezifikation verweist grundsätzlich auf die Ausführungen im ES/TS 101 671.	Die genaue Ausgestaltung der Überwachungseinrichtung, insbesondere die Events mit den zugehörigen Parametern, muss mit der Bundesnetzagentur abgestimmt werden.
Annex A	**ASN.1-Module** Das verwendete Modul ' TS101909202' enthält Syntaxfehler.	Eine berichtigte Version steht unter http://www.bundesnetzagentur.de/tku zur Verfügung.
Zusatz 1	**Target Identity** Es gelten grundsätzlich die Vorgaben nach Abschnitt 6 der TR TKÜV.	Eine Umsetzung der Überwachung auf der Basis der MAC Adresse eines Modems ist grundsätzlich möglich, doch muss berücksichtigt werden, dass an den zu überwachenden Internetzugangsweg ein anderes Modem angeschaltet werden kann oder das "überwachte" Modem an einen anderen Internetzugangsweg angeschaltet werden kann.
Zusatz 2	**Timestamps** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) anzugeben	Die Kodierung des Parameters GeneralizedTime erfolgt als universal time und ohne time difference.

Anlage G.2 Erläuterungen zu den ASN.1-Beschreibungen

Die Bundesnetzagentur informiert gemäß § 11 Satz 5 TKÜV auf ihrer Internetseite über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage G sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-01, TS 102 232-03, TS 102 232-04 und TS 101 909-20-2 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung von FTP als Übertragungsprotokoll sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in den Spezifikationen als 'conditional’ und 'optional’ bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach Anlage G.1 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, z.B. ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder z.B. DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

Die Übermittlung administrativer Ereignisse (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme sowie Fehlermeldungen) sowie zusätzlicher Ereignisse (z.B. bezüglich herstellereigener Dienste) erfolgt nach Anlage A.3.

Anlage H Festlegungen für VoIP und sonstige Multimediadienste (ETSI TS 102 232-05, -06 und 101 909-20-1)

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt nach den ETSI-Spezifikationen TS 102 232-05 [34] für IP-Multimedia-Dienste und TS 101 909-20-1 für die IP-Cablecom-Architektur sowie nach der ETSI-Spezifikation TS 102 232-06 [35] für emulierte PSTN/ISDN-Dienste. Die ETSI-Spezifikation nutzt den generellen IP-basierten Übergabepunkt, der in der ETSI-Spezifikation TS 102 232-01 [29] beschrieben ist.

Bisher war es auch für VoIP-Dienste zulässig, die Überwachungstechnik auf der Grundlage der in Anlage C beschriebenen leitungsvermittelten Technik zu gestalten. Die Nutzung dieser Schnittstelle, auch für darüber hinausgehende Multimediadienste, ist für neue Implementierungen künftig nicht mehr möglich. Bezüglich bestehender Implementierungen müssen die in Anlage C beschriebenen Fristen beachtet werden.

Angebote von VoIP bzw. sonstigen Multimediadiensten innerhalb von GPRS- und UMTS-Netzen bleiben von dieser Anlage grundsätzlich unberührt, da die Anlage D diesbezüglich bereits Übergabepunkte beschreibt.

Die Anlage beinhaltet die Entscheidung über die in den Spezifikationen enthaltenen Optionen und die Festlegungen ergänzender technischer Anforderungen.

Neben den Anforderungen nach Teil A, Abschnitte 3 und 4, sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.2	Teilnahme am VPN mittels Kryptobox. Da die Übermittlung der Überwachungskopie per TCP/IP über das Internet erfolgt, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage H.1 Grundsätzliche Anforderungen bei Anwendung von ´Service-specific details for IP Multimedia Services (TS 102 232-05 bzw. TS 101 909-20-1)

Die ETSI-Spezifikation TS 102 232-05 beschreibt einen Übergabepunkt für VoIP und sonstige Multimediadienste, die auf dem Session Initiation Protocol (SIP), den ITU-T Standards H.323 und H.248 sowie dem Realtime Transport Protocol (RTP) beruhen.

Die ETSI-Spezifikation TS 101 909-20-1 kann bei Netzen nach der IP-Cablecom-Architektur eingesetzt werden.

Anlage H.1.1 Begriffsbestimmungen

Multimedia-Server (VoIP-Server) und beteiligte Netzelemente	An der Erbringung des Dienstes VoIP oder eines sonstigen Multimediadienstes beteiligten Telekommunikationsanlagen, die auf SIP, H.323 oder H.248 in Verbindungen mit dem media stream (z.B. RTP) beruhen.
VoIP-Kennung	Die VoIP-Kennung bezeichnet die zu überwachende Telekommunikation. Der Begriff wird stellvertretend für die verschiedenen Arten möglicher Kennungen verwendet.
VoIP-Account	Zur gemeinsamen Organisation mehrerer VoIP-Kennungen für den Nutzer eingerichteter Account. Ein zu überwachender VoIP-Account kann u.U. mehrere VoIP-Kennungen beinhalten.
Login	Vorgang, bei der die Zugangsberechtigung eines Teilnehmers oder sonstigen Endnutzers zu seinem VoIP-Account geprüft wird.
Login-Name	Der beim Login als Teil der Zugangskennung verwendete Login-Name ist ebenfalls eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

Anlage H.1.2 Grundsätzliches

In einer Anordnung zur Überwachung der Telekommunikation kann als technisches Merkmal

- eine VoIP-Kennung oder
- die Zugangskennung (Login-Name ohne Passwort) eines VoIP-Accounts genannt werden.

Um die Überwachung der vollständigen Telekommunikation, die über eine VoIP-Kennung abgewickelt wird, durchzuführen, muss sichergestellt werden, dass die überwachte Telekommunikation tatsächlich dem züA durch die Verwendung von geeigneten Authentifizierungsmethoden zuzuordnen ist. Dadurch soll beispielsweise verhindert werden, dass eine zu überwachende VoIP-Kommunikation nur deswegen nicht erfasst wird, weil die Absenderadresse durch den Nutzer manipuliert wurde.

Kann diese Anforderung (z.B. wegen einer ungeeigneten Authentifizierungsmethode) nicht erfüllt werden, muss eine auf eine VoIP-Kennung bezogene Anordnung ersatzweise durch die Überwachung des gesamten VoIP-Accounts durchgeführt werden, bei der die Telekommunikation jeder VoIP-Kennung dieses Accounts erfasst werden muss.

Besteht bereits zum Zeitpunkt der Aktivierung einer Überwachungsmaßnahme eine Telekommunikationsverbindung mit der überwachten Kennung, muss der Telekommunikationsinhalt sowie die Ereignisdaten ab diesem Zeitpunkt erfasst und als Kopie bereitgestellt werden (siehe hierzu Anlage H.3.2 Punkt 5.3). Daten nach § 7 Abs. 1 TKÜV, die zum Zeitpunkt der Aktivierung der Überwachungsmaßnahme im Netz vorhanden sind und nicht mehr über künftige Ereignisdaten ausgeleitet werden (z. B. Codecs der bestehenden Telekommunikation), müssen ebenfalls berichtet werden. Diese Anforderung ist bis spätestens zum 31.12.2017 umzusetzen.~~Ereignisdaten, beispielsweise bezüglich der beteiligten Kennungen und der verwendeten Kodierung der Nutzinformation, sind nach § 7 Abs. 1 TKÜV auch dann zu berichten, wenn diese nicht in der Signalisierung übermittelt werden, aber für diesen Telekommunikationsvorgang anderswo im Netz des verpflichteten (z.B. in einem Netzelement) verfügbar sind.zum~~

Anlage H.1.3 Vollständigkeit der Ereignisdaten

Bei der Verwendung der beiden o.g. ETSI-Spezifikationen wird davon ausgegangen, dass die für den Dienst genutzten Signalisierungsinformationen ausreichend sind, um die zu überwachenden Ereignisse zu beschreiben. Kann dies nicht erreicht werden, müssen die Ereignisdaten über das Modul HI2Operations aus der Anlage C übermittelt werden, welches neben der Übermittlung der Kopie der SIP-Signalisierung weitere Parameter enthält, um fehlende Informationen zu ergänzen. Solche Informationen können beispielsweise in Netzelementen (z.B. SIP-Proxy, Konferenzserver, Web-Interface für Nutzereinstellungen) bekannt sein.

Bei der Gestaltung der Überwachungstechnik muss darauf geachtet werden, dass jede der zu der überwachenden Kennung zugeordneten Signalisierungsnachricht entsprechend § 5 Abs. 1 TKÜV erfasst wird. Zur Vermeidung einer mehrfachen Erfassung von Signalisierungsnachrichten, ohne dass dadurch weitere Details zu den nach § 7 TKÜV definierten Ereignisdaten (z.B. Kennungen, genutzte Dienste) bekannt werden, muss die Anzahl der eingesetzten Überwachungspunkte auf das notwendige Minimum begrenzt werden. Dadurch soll beispielsweise die mehrfache Erfassung einer INVITE-Nachricht an verschiedenen Verbindungsknoten (Hops) innerhalb des Netzes vermieden werden, in denen lediglich die Information des Hops hinzugefügt ist. Eine Logik zur Filterung und ggf. Unterdrückung der an den Überwachungspunkten erfassten Nachrichten vor der Bereitstellung am Übergabepunkt ist jedoch nicht erforderlich.

Anlage H.1.4 Bereitstellung der Nutzinformationen bei getrennter Übermittlung von der Signalisierung

Grundsätzlich müssen die auf der Grundlage der Signalisierung erzeugten Ereignisdaten und die Nutzinformationen am Übergabepunkt bereitgestellt werden. Nach der ETSI-Spezifikation TS 102 232-05 bestehen die Nutzinformationen aus der Gesamtheit der RTP und RTCP-Pakete sowie möglichen weiteren Protokollen, die den media stream transportieren (z.B. Gateway-Protokolle). Insbesondere bei VoIP werden die Nutzinformationen jedoch teilweise getrennt von der Signalisierung durch andere Betreiber übermittelt. Zur Bereitstellung der Nutzinformationen stehen folgende Möglichkeiten zur Verfügung:

1. Der VoIP-Anbieter betreibt selbst Netzelemente, über die Nutzinformation übermittelt werden. Diese Netzelemente können sein:

   a) der Internetzugangsweg, unabhängig davon, ob dieser auf einer eigenen oder angemieteten Teilnehmeranschlussleitung beruht (hierzu zählen jedoch keine vollständigen Resale-Produkte z.B. Resale DSL der DTAG),

   b) der Netzknoten, der den Koppelpunkt zum Internet enthält,

   c) das Transport- bzw. Verbindungsnetz für Nutzinformationen oder

   d) der Übergabepunkt vom/zum PSTN (z.B. Media-Gateway).

   Hierfür schreibt diese Anlage H die näheren Anforderungen vor.

2. Der VoIP-Anbieter bedient sich eines bestimmten Betreibers von Netzelementen nach 1. zur Übermittlung der Nutzinformation. Hierfür steht zusätzlich zu Vorgaben der Anlage H eine Möglichkeit der Umsetzung gemäß § 110 Abs. 1 Satz 1 Nr. 1a TKG zur Verfügung. Die Umsetzung der entsprechenden Zusammenwirkung obliegt jedoch dem verpflichteten VoIP-Anbieter.

Werden die Nutzinformationen sowie die Ereignisdaten getrennt bereitgestellt, ist gemäß § 7 Abs. 2 TKÜV darauf zu achten, dass diese Anteile mit einer einheitlichen Referenznummer sowie der Zuordnungsnummer gekennzeichnet werden.

Soll die Überwachung der Nutzinformation durch ein spezielles Routing, z.B. zu einem zentralen Netzknoten erfolgen, muss besonders darauf geachtet werden, dass dies gemäß § 5 Abs. 4 TKÜV nicht durch die VoIP-Teilnehmer festgestellt werden kann.

Anlage H.2 Grundsätzliche Anforderungen bei Anwendung von ´Service-specific details for PSTN/ISDN services´ (ETSI TS 102 232-06)

Die ETSI-Spezifikation TS 102 232-06 eröffnet für emulierte PSTN- und ISDN-Dienste die Möglichkeit der Nutzung eines rein IP-basierten Übergabepunktes. Dabei wird die Kopie der Telekommunikation als RTP-Datenstrom über den generellen IP-basierten Übergabepunkt nach TS 102 232-01 übermittelt. Zudem werden die Ereignisdaten, die nach Anlage C im Modul HI2Operatons kodiert sind, ebenfalls mit dem TS 102 232-01 übermittelt; die FTP-Übermittlungsmethode nach Anlage C muss hierbei nicht angewendet werden.

Anlage H.3 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage H.3.1 Grundlage: ETSI TS 102 232-01

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-01 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-01	**Beschreibung der Option bzw. des Problempunktes,** **Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1-Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als *delivery country code* 'DE' zu verwenden. Der *operator identifier* wird nach Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der *network element identifier* ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die *communication identity number* kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Abs. 2 Satz 2 TKÜV vorgesehenen Zuordnungsnummer. ~~Zu beachten ist:~~ • ~~Die CIN ist nur innerhalb eines überwachenden Netzelementes einheitlich, in Mobilfunknetzen kann sich die CIN nach Standortwechsel wiederholen. Zur Trennung muss zusätzlich der Interception Point Identifier herangezogen werden~~ • ~~Wechselt der Nutzer während eines Gesprächs den Standort kann eine Korrelation ohne Zusatzauswertung (z.B. zeitlicher Bezug) nicht mehr hergestellt werden (unterschiedliche CIN und unterschiedlicher Interception Point Identifier)~~
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam vermeiden und die Reihenfolge sicherstellen.

Abschnitt TS 102 232-01	**Beschreibung der Option bzw. des Problempunktes,** **Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
5.2.6	**Payload timestamp** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) als~~:~~ ~~*GeneralizedTime* sowie im Format des~~ *MicroSecondTimeStamp* (mit höchster Auflösung und Genauigkeit) anzugeben. Der *MicroSecondTimeStamp* muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	Mit der TR TKÜV, Ausgabe 7.0 ist nur noch der *MicroSecondTimeStamp zu verwenden.* Ist der Zeitstempel nicht im Format des *MicroSecondTimeStamp* am Interceptionpoint verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren. ~~Die Kodierung des Parameters *GeneralizedTime* erfolgt als universal time und ohne time difference.~~ ~~Die zusätzliche Zeitangabe als *MicroSecondTimeStamp* soll insbesondere in Fehlerfällen die Rekonstruktion der Teillieferungen ermöglichen.~~
5.2.7	**Payload direction** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzdaten mit *to target* bzw. *from target* zu erfolgen.	
	Kodierungsinformation Dem Endgerät stehen in der Regel verschiedene optional nutzbare Kodierungen der Audiodaten zur Verfügung. Der für die Übertragung der Audiodaten tatsächlich genutzte und dem Netz bekannte Codec muss gemäß § 7 Abs. 1 TKÜV als Ereignisdatum übermittelt werden. (Der Hinweis auf die bestehende Rechtslage wurde aufgrund der Verwendung unterschiedlicher, teils dem Auswertesystem unbekannter Codecs in die TR TKÜV aufgenommen.)	Grundsätzlich ist der genutzte Codec (wenn dem Netz bekannt) bei einfacher Ausleitung der IRI-Daten, als Ereignisdatum zu berichten. Werden die IRI Daten an verschieden Punkten im Netz erfasst und kommt es dabei ggf. zur Ausleitung verschiedener Codecs (z.B. Codecwechsel im Netz) so soll der *Interception Point Identifier* dabei helfen, den relevanten IRI-Datensatz mit den ausgeleiteten Nutzinformationen (Audiodaten) zusammenzuführen (siehe Punkt 5.2.11).
5.2.11	**Interception Point Identifier** Der interception point identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.~~logischen ,/oder~~	Der *Interception Point Identifier* soll dabei unterstützen, bei einer mehrfachen Ausleitung von IRI-Daten (z.B. durch unterschiedliche Erfassungspunkte) die zusammengehörigen IRI-Daten besser zu kennzeichnen und, falls möglich, den über den IRI-Datensatz beschriebenen Codec mit den ausgeleiteten Nutzinformationen (Audiodaten) zusammenzuführen Die Umsetzung dieser Forderung soll wie folgt erfolgen, wenn mehrere Codecs in den IRI-Daten berichtet werden: Erfolgt innerhalb des Netzes ein Wechsel des Codecs der Audiodaten, so sollten die auszuleitenden CC-Daten mit dem gleichen Interception Point Identifier versehen sein wie der dazugehörige IRI-Datensatz, der den korrekten Codec enthält. Sollte die oben beschrieben Korrelation nicht möglich sein, so sind alternative Maßnahmen mit der Bundesnetzagentur abzustimmen.

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
	~~**Kodierungsinformation**~~ ~~Stehen dem Nutzer verschiedene Kodierungen der Nutzinfomrationen zur Verfügung, müssen diese nach § 7 Abs. 1 TKÜV als Ereignisdaten übermittelt werden. Dies muss so eindeutig erfolgen, dass der berichtete Codec eindeutig der ausgeleiteten Kopie der Nutzinformation entspricht. (Der Hinweis auf die bestehende Rechtslage wurde aufgrund der Verwendung unterschiedlicher Codecs in die TR TKÜV aufgenommen.)~~	~~Die Umsetzung dieser Forderung soll wie folgt erfolgen, wenn mehrere Codecs in den IRI-Daten berichtet werden:~~ ~~Erfolgt innerhalb des Netzes ein Wechsel des Codecs der Audiodaten, so sollten die auszuleitenden CC-Daten mit dem gleichen Interception Point Identifier versehen sein wie der dazugehörige IRI-Datensatz, der den korrekten Codec enthält.~~
6.2.2	**Error Reporting** Die Übermittlung richtet sich grundsätzlich nach Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist grundsätzlich vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem maßnahmenbezogenen Einsatz von Padding muss die jeweilige bS zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt grundsätzlich Abschnitt ~~5.1~~3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der bS zu verhindern.	
6.3.4	**Keep-alives** Kann optional vom Verpflichteten implementiert werden. Für die verpflichtende Verwendung von *Keep-Alives* sind die Vorgaben der grundsätzlichen Anforderungen aus Teil A, Punkt 3.3 zu beachten.	Grundsätzlich muss die TCP-Verbindung nach erfolgreicher Übermittlung von Daten timer-gesteuert abgebaut werden. Dem maßnahmenbezogenen Einsatz von Keep-alives, bei der die TCP-Verbindung ständig aufrechterhalten bleibt, muss die jeweilige bS zustimmen.
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der bS (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 und TS 102 232-06.
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	

Abschnitt TS 102 232-01	**Beschreibung der Option bzw. des Problempunktes,** **Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
7.2	**Security requirements** Es gelten die Anforderungen nach Anlage A.2 der TR TKÜV.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden.
7.3.2	**Timeliness** Eine eventuelle Nutzung separater *managed networks* ist zwischen dem Verpflichteten und den bSn abzustimmen.	

Anlage H.3.2 Grundlage: ETSI TS 102 232-05

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-05 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-05	**Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
4.3	**General Requirements** Grundsätzlich werden die Kopien der Signalisierungsinformationen (z.B. SIP Messages) als Ereignisdaten übermittelt. Ereignisdaten, die nicht Teil der Signalisierung sind, müssen ergänzend übermittelt werden. Ein generelles Mapping, wie z.B. nach ANS T1.678 ist nicht vorgesehen.	Im Konzept müssen die für die verschiedenen Einzeldienste (z.B. basic call, call forwarding) bezeichnenden Parameter bzw. Kombinationen der Messages beispielhaft erläutert werden. Einzeldienste, die durch die Endgeräte (Clients) der Teilnehmer gesteuert werden können, müssen, soweit bekannt, ebenfalls im Hinblick auf ein verändertes Verhalten in der Signalisierung oder den RTP-Streams (z.B. gleichzeitige RTP-Sessions bei Konferenzen) erläutert werden; spätere Erweiterungen müssen nachgeführt werden. Für die Übermittlung sämtlicher Ereignisdaten ist das Modul HI2Operatons aus der Anlage C zu verwenden, wobei für die SIP-Messages ein eigener Parameter genutzt werden kann; das Modul wird nach den Vorgaben des TS 101 232-06 übertragen.
5.2.5	**Provisioning of the H.323 IRI IIF** Welche Signalisierungsnachrichten der verschiedenen Protokolle der H.323-Familie als Ereignisdaten übermittelt werden müssen, ist mit der Bundesnetzagentur im Einzelfall zu erörtern.	
5.3	**Assigning a value to the CIN** Grundsätzlich wird die CIN bei einer neuen session mit der ersten Signalisierungsinformation (CC oder IRI) vergeben. Besteht bei der Aktivierung der Überwachungs-maßnahmen bereits eine session, muss die CIN mit der ersten IRI- oder CC-Message generiert werden.	Die erste Signalisierungsinformation (z.B. INVITE) muss als IRI-BEGIN, alle weiteren Signalisierungsinformationen (z.B. z.B. INVITE vom SIP-Server zur Partnerkennung) müssen als IRI-CONTINUE gekennzeichnet werden. Die letzte (erwartete) Signalisierungsinformation wird als IRI-END gekennzeichnet. Besteht bereits zum Zeitpunkt der Aktivierung einer Überwachungsmaßnahme eine Telekommunikationsverbindung mit der überwachten Kennung, muss der Telekommunikationsinhalt sowie die Ereignisdaten ab diesem Zeitpunkt erfasst und als Kopie bereitgestellt werden.

Abschnitt TS 102 232-05	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.3., 5.3.1	**Assigning a CIN value to SIP related IRI** Die Beschreibung geht von der Nutzung der Call-ID sowie des "O"-Feldes des SDP aus, um für den gesamten call eine einheitliche CIN (Zuordnungsnummer) zu generieren.	Unabhängig davon, ob die beschriebenen Parameter genutzt werden können, gilt die Anforderung zur Generierung einer einheitlichen CIN für die einzelnen communication sessions. Für die Behandlung verschiedener media streams innerhalb einer session muss ggf. der stream identifier nach Abschnitt 5.5 verwendet werden.
5.4	**Events and IRI record types** Die verschiedenen gesprächsbezogenen Ereignisdaten werden als IRI-BEGIN, IRI-CONTINUE und IRI-END berichtet; ein nachträgliches Event (nach einem IRI-END) wird wie beschrieben als IRI-REPORT berichtet.	Die Option, alle Ereignisdaten als REPORT zu senden, ist nicht erlaubt. In bestimmten, vorher mit der Bundesnetzagentur abzustimmenden Ausnahmefällen, ist es erlaubt, Daten einer bestehenden Session teilweise als REPORT zu berichten. (Dies kann z.B. ein Rufweiterleitungsszenario sein, bei dem die Session zunächst als BEGIN/CONTINUE/END und nach der Weiterleitung als REPORT berichtet wird.) Nur je ein Event einer session darf als IRI-BEGIN bzw. IRI-END bezeichnet werden. D.h. die erste Signalisierungsinformation (z.B. INVITE) wird als IRI-BEGIN, alle weiteren Signalisierungs-informationen (~~z.B.~~ z.B. INVITE vom SIP-Server zur Partnerkennung) werden als IRI-CONTINUE gekennzeichnet. Die letzte (erwartete) Signalisierungsinformation wird als IRI-END gekennzeichnet.
5.5	**Interception of Content of Communication** Wird Verschlüsselung netzseitig eingesetzt, muss diese am Übergabepunkt aufgehoben werden (§ 8 Abs. 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss. Der stream identifier muss bei mehreren media streams innerhalb einer session verwendet werden.	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente bzw. die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der bS übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden. Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.

Abschnitt TS 102 232-05	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
7	**ASN.1 specification for IRI and CC** Mit den Parametern ìPSourceAddress´ und ´iPDestinationAddress` sind die aus Sicht des Netzes des Verpflichteten bekannten IP-Adressen der Kommunikationspartner zu übermitteln. Kann keine Angabe zum Standort des Endgerätes gemäß § 7 Abs. 1 Nr. 7 TKÜV berichtet werden, dient diese IP-Adresse zudem als Standortangabe. Diese Übergangslösung gilt, bis die Übermittlung einer konkreten Standortangabe verfügbar ist.	Das Berichten interner IP-Adressen des Netzes, z.B. wenn die IP-Adressen der Kommunikationspartner zwar an den Netzgrenzen, jedoch nicht unmittelbar am VoIP-Server vorliegen, entspricht nicht der Regelung.

Anlage H.3.3 Grundlage: ETSI TS 101 909-20-1

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 101 909-20-1 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 101 909-20-1	**Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
	Ereignisdaten, die nicht Teil der Signalisierung sind, müssen ergänzend übermittelt werden.	Im Konzept müssen die für die verschiedenen Einzeldienste (z.B. basic call, call forwarding) bezeichnenden Parameter bzw. Kombinationen der Messages beispielhaft erläutert werden. Einzeldienste, die durch die Endgeräte (Clients) der Teilnehmer gesteuert werden können, müssen, soweit bekannt, ebenfalls im Hinblick auf ein verändertes Verhalten in der Signalisierung oder den RTP-Streams (z.B. gleichzeitige RTP-Sessions bei Konferenzen) erläutert werden; spätere Erweiterungen müssen nachgeführt werden. Für die Übermittlung sämtlicher Ereignisdaten ist das Modul HI2Operatons aus der Anlage C zu verwenden, wobei für die Signalisierungs-Messages ein eigener Parameter genutzt werden kann; das Modul wird nach den Vorgaben des TS 101 232-06 übertragen.
5	**Functional Archtitecture** Es wird eine Implementierung auf der Grundlage des EuroDOCSIS vorausgesetzt	Abhängig von der Gestaltung der TKA-V, insbesondere des Diensteumfangs, kann die Bundesnetzagentur eine bestimmte Version des Standards vorgeben.
5.2	**Functional Components** Die Spezifikation verweist grundsätzlich auf die Ausführungen im ES 201 671 bzw. TS 101 671.	Die genaue Ausgestaltung der Überwachungseinrichtung, insbesondere die Events mit den zugehörigen Parametern, muss mit der Bundesnetzagentur abgestimmt werden.
4.4	**Interworking Considerations** Wird Verschlüsselung netzseitig eingesetzt, muss diese am Übergabepunkt aufgehoben werden (§ 8 Abs. 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss.	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente bzw. die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der bS übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden. Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
Annex A	**ASN.1-Module** Die verwendeten Module 'PCESP' und 'TS101909201' enthalten Syntaxfehler.	Eine berichtigte Version steht unter http://www.bundesnetzagentur.de/tku zur Verfügung.

Abschnitt TS 101 909-20-1	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
Zusatz 1	**ASN.1 specification for IRI and CC** Bei Verwendung dieser Schnittstelle müssen die IP-Adressen der Kommunikationspartner berichtet werden.	Siehe hierzu die Hinweise zu Kapitel 7 in der Beschreibung zur Verwendung der Schnittstelle nach TS 102 232-05 in Anlage H.3.2.
Zusatz 2	**Timestamps** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) anzugeben	Die Kodierung des Parameters GeneralizedTime erfolgt als universal time und ohne time difference.

Anlage H.3.4 Grundlage: ETSI TS 102 232-06

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-06 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-06	**Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
5.2	**Structures** • Die Ereignisdaten werden mit dem Modul HI2Operations nach Anlage C kodiert und mittels des Parameters *ETSI671IRI* direkt mit TS 101 232-01 übermittelt. • Die Kopie der Nutzinformation werden als RTP-Pakete mit UDP- und IP-Header mittels des Parameters *PstnIsdnCC* über den TS 102 232-06 mit dem TS 102 232-01 übermittelt. • Die zur Interpretierung der RTP-Pakete notwenigen Informationen werden ebenfalls mit dem Paramater PstnIsdnIRI über den TS 102 232-06 mit dem TS 102 232-01 übermittelt.	
6.2	**CC format** Wird Verschlüsselung netzseitig eingesetzt, muss diese am Übergabepunkt aufgehoben werden (§ 8 Abs. 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss.	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente bzw. die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der bS übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
6.2, 6.3.2	**Supplementary information** Es soll standardmäßig G.711 eingesetzt werden (mediaAttributes = "1") Es soll immer die Kopie der gesamten SDP-Message im Feld *copyOfSDPMessage* übermittelt werden (mandatory); die optionalen Einzelfelder *sessionName* und *sessionInfo* werden nicht benötigt (optional).	Durch die Übermittlung der gesamten SDP-Message erhält die bS die vollständige Kopie der Telekommunikation; zudem werden Fehler beim Herauskopieren einzelner Parameter seitens des Verpflichteten vermieden.
Ergänzung 1	**ASN.1 specification for IRI and CC** Bei Verwendung dieser Schnittstelle müssen die IP-Adressen der Kommunikationspartner berichtet werden.	Siehe hierzu die Hinweise zu Kapitel 7 in der Beschreibung zur Verwendung der Schnittstelle nach TS 102 232-05 in Anlage H.3.2.

Anlage H.4 Erläuterungen zu den ASN.1-Beschreibungen

Die Bundesnetzagentur informiert gemäß § 11 Satz 5 TKÜV auf ihrer Internetseite über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage H sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-01, TS 102 232-05, TS 102 232-06 sowie TS 101 909 20-1 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung von FTP als Übertragungsprotokoll sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in den Spezifikationen als 'conditional’ und 'optional’ bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach Anlage H.2 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, z.B. ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder z.B. DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

Die Übermittlung administrativer Ereignisse (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme sowie Fehlermeldungen) sowie zusätzlicher Ereignisse (z.B. bezüglich herstellereigener Dienste) erfolgt nach Anlage A.3.

Teil B

Technische Umsetzung gesetzlicher Maßnahmen zur Erteilung von Auskünften

1 Grundsätzliches

Dieser Teil B der TR TKÜV beschreibt auf der Grundlage des § 110 Abs. 3 TKG [21] i.V.m. §§ 96, 113 Abs. 5 und 113c Abs. 3 TKG die

1. technischen Einzelheiten, die im Zusammenhang mit Auskunftersuchen der berechtigten Stellen und der Erteilung von Auskünften über Bestands- und Verkehrsdaten durch die verpflichteten Diensteanbieter und Netzbetreiber zu beachten sind, ~~sowie~~
2. die technischen Eigenschaften der erforderlichen Sende- und Empfangsanschlüsse der Verpflichteten sowie der berechtigten Stellen, sowie
3. die Anforderungen zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität nach § 113f Abs. 1 TKG bei der Übermittlung von speicherpflichtigen Verkehrsdaten nach §113c Abs. 3 Satz 1 TKG,

Die technischen Einzelheiten, die bis zum Inkrafttreten einer entsprechender TKÜV-Neuregelung (nachfolgend zur Unterscheidung zur derzeit gültigen TKÜV als TKÜV-Neu bezeichnet) schon jetzt optional umgesetzt werden können, aber mit Inkrafttreten der TKÜV-Neu – unter Berücksichtigung der gesetzlich geregelten Übergangsfristen – verpflichtend werden, werden nachfolgend bereits beschrieben. Insbesondere wird auf die im Teil 4 der TKÜV-Neu benannten Verpflichtungen zu Vorkehrungen für die Erteilung von Auskünften über Verkehrsdaten eingegangen.

Zudem werden weitere optionale Nutzungsmöglichkeiten der Schnittstelle beschrieben, die der Effektivität des Gesamtverfahrens dienen.

Dieser Teil beschreibt darüber hinaus die technischen Einzelheiten~~das Verfahren~~ zur gesicherten elektronischen Übermittlung von Anordnungen zur Beauskunftung von Verkehrsdaten und~~,~~ zur Überwachung der Telekommunikation nach § 12 Abs. 2 TKÜV-Neu sowie für sonstige Nutzungen. ~~Bei Nutzung dieses Verfahrens ist die Nachlieferung des Originals oder einer beglaubigten Abschrift nicht erforderlich. Unternehmen, die nach der TKÜV verpflichtet sind, an dem Verfahren teilzunehmen, haben auch die hier beschriebene gesicherte elektronische Schnittstelle zu betreiben.~~

Die in diesem Teil B der TR TKÜV~~hier~~ beschriebenen~~, gesicherte Übermittlungsverfahren~~~~Schnittstelle~~ m~~ü~~üssen bzw. k~~a~~önnen (Kennzeichnung „optional“) zu folgenden Zwecken genutzt werden:

a. Erteilung von Auskünften über Bestandsdaten gemäß § 113 Abs. 5 Satz 2 TKG,
b. Übermittlung der Anordnung zum Auskunftersuchen von Verkehrsdaten ~~und sonstigen Nutzungen~~ (optional bis zum Inkrafttreten der TKÜV-Neu, danach verpflichtend),
c. Erteilung von Auskünften über Verkehrsdaten nach § 96 TKG ~~den §§ 96 und 113b TKG, z.B. nach § 100g StPO~~ (optional bis zum Inkrafttreten der TKÜV-Neu, danach verpflichtend),
d. Erteilung von Auskünften über Verkehrsdaten nach § 113b TKG (optional bis zum Inkrafttreten der TKÜV-Neu, danach verpflichtend),
e. Erteilung von Auskünften über Verkehrsdaten nach § 96 TKG in Echtzeit~~, z.B. nach § 100g Abs. 1 Satz 3 StPO~~ (optional bis zum Inkrafttreten der TKÜV-Neu, danach verpflichtend),
f. Erteilung von Auskünften über die Struktur von Funkzellen[1] (optional),
g. Erteilung von Auskünften zur Standortfeststellung von mobilen Endgeräten (optional),
h. Übermittlung der Anordnung zur Überwachung der Telekommunikation (optional bis zum Inkrafttreten der TKÜV-Neu, danach verpflichtend),
i. Übermittlung von Daten zum Rechnungsabgleich im Vorfeld der Entschädigung nach § 23 Absatz 1 JVEG (optional).

[1] Funkzelle im Sinne dieser Richtlinie ist der Bereich, den ein Mobilfunkantennenelement, dem ein eigenes Identifizierungsmerkmal (Cell Identifier) zugewiesen ist, funktechnisch abdeckt.

Zur besseren Lesbarkeit wird in dieser TR TKÜV alternativ auch der Begriff „Beauskunftung“ synonym für die Erteilung der Auskunft (response) als auch für den Auftrag zur Erteilung von Auskünften (request) verwendet.

2 Übermittlungsverfahren ETSI-ESB und E-Mail-ESB

Die in den nachfolgenden Anlagen A und B beschriebenen Übermittlungsverfahren müssen nach Teil 4 der TKÜV-Neu (optional bis zum Inkrafttreten der TKÜV-Neu, danach verpflichtend) wie folgt eingesetzt werden:

- Das Übermittlungsverfahren ETSI-ESB (Anlage A) muss zur Erteilung von Auskünften über Bestandsdaten und Verkehrsdaten sowie zur Entgegennahme entsprechender Anordnungen von denen nach § 113 Abs. 5 Satz 2 TKG Verpflichteten eingesetzt werden.

  Andere nach dem Teil 4 der TKÜV-Neu Verpflichtete können dieses Übermittlungsverfahren alternativ zu dem Übermittlungsverfahren E-Mail-ESB einsetzen, wobei einem Mischbetrieb für verschiedene Anwendungen (z.B. ETSI-ESB für Verkehrsdatenauskünfte inkl. Übermittlung der zugehörigen Anordnung und E-Mail-ESB für Auskünfte zu Bestandsdaten) nach Absprache mit der Bundesnetzagentur zugestimmt werden kann.

- Das Übermittlungsverfahren E-Mail-ESB (Anlage B) muss zur Beantwortung von Auskunftsersuchen über Verkehrsdaten nach dem Teil 4 der TKÜV-Neu von denjenigen Verpflichteten eingesetzt werden, die nicht nach § 113 Abs. 5 Satz 2 TKG verpflichtet sind.

  Die Verpflichteten können alternativ das Übermittlungsverfahren ETSI-ESB nach Maßgabe der obigen Regelung einsetzen.

Diese Übermittlungsverfahren können für die sonstigen Nutzungen nach Abschnitt 1 genutzt werden.

Das bisher noch genutzte verschlüsselte Übermittlungsverfahren ESB kann nach Abstimmung mit der Bundesnetzagentur alternativ zur E-Mail-ESB zusätzlich vorgehalten werden, soweit die bezüglichense ~~grundsätzlichen~~ Anforderungen gleichermaßen eingehalten werden. Andere Übermittlungsverfahren sowie eine Übergabe vor Ort sind ausgeschlossen, wenn die Systeme auch für die Beauskunftung von Verkehrsdaten nach § 113b TKG vorgehalten werden.

Unsichere Übermittlungsverfahren, beispielsweise die unverschlüsselte Übertragung per E-Mail oder die postalische Versendung von unverschlüsselten Datenträgern, sind grundsätzlich, d.h. auch außerhalb der Verwendung der vorgehaltenen Systeme zur Beauskunftung von Verkehrsdaten nach § 113b TKG unzulässig.

Diese Vorgaben gelten nach § 1 Abs. 1 Nr. 7 TKÜV entsprechend für die Aufzeichnungsanschlüsse der berechtigten Stellen, auch bei Mitbenutzung zentraler Eingangsschnittstellen. Zudem ist der Betrieb der E-Mail-ESB außerhalb der bSn, der Verpflichteten oder deren Erfüllungsgehilfen nicht zulässig.

3 Gewährleistung von Datensicherheit und Datenqualität

3.1 Grundsätzliche Anforderungen

Grundsätzlich gelten die Vorgaben nach § 14 Abs. 1 TKÜV, wonach der Verpflichtete die von ihm getroffenen technischen und organisatorischen Vorkehrungen zur Umsetzung von Maßnahmen sowie die Übermittlung an die Empfangsee~~r~~inrichtung der berechtigten Stelle nach dem Stand der Technik gegen unbefugte Inanspruchnahme zu schützen hat.

Die Übermittlung an die bS muss ~~insbesondere~~ verschlüsselt erfolgen; die Verfahren dazu werden in den nachfolgenden Beschreibungen der Übermittlungsverfahren vorgegeben.

Die Vorgaben des § 14 Abs. 3 TKÜV gelten ebenso für die Administration von Netzelementen über öffentliche Netze zur Überwachung bzw. zum Abruf von Auskunftsdaten inkl. der Speicherung von hierzu notwendigen Informationen in diesen Netzelementen. Bei der

Umsetzung dieser Anforderungen sind hierzu erarbeitete internationale Standards sowie die Empfehlungen des BSI zu berücksichtigen.

~~Bezüglich der Datenqualität der übermittelnden Überwachungskopien und Auskünfte gilt die Regelung nach § 8 Abs. 2 Nr. 3 TKÜV.~~

3.~~1~~2 Besondere Anforderungen an die Übermittlung von speicherpflichtigen Verkehrsdaten nach § 113b TKG

Nach § 113c Abs. 3 Satz 1 i.V.m. § 113f Abs. 1 Satz 1 TKG ist bei der Übermittlung von Verkehrsdaten nach § 113b TKG ein besonders hoher Standard der Datensicherheit und Datenqualität zu gewährleisten.

Die Bundesnetzagentur hat gemeinsam mit BSI und BfDI den Anforderungskatalog nach § 113f TKG erarbeitet, bei dessen Einhaltung vermutet wird, dass die gesetzlichen Anforderungen nach den §§ 113b bis 113e TKG eingehalten werden.

Diese nachfolgenden besonderen Anforderungen gelten für die hierfür betriebenen Übermittlungsverfahren, sofern diese

- ausschließlich für die Erteilung von Auskünften über Verkehrsdaten nach § 113b TKG oder
- neben anderen nach obigem Abschnitt 1 erlaubten Nutzungsformen auch für die Erteilung von Auskünften über Verkehrsdaten nach § 113b TKG genutzt werden.

Das nachfolgende Bild aus dem Anforderungskatalog zeigt eine mögliche Umsetzung der Gesamtarchitektur:

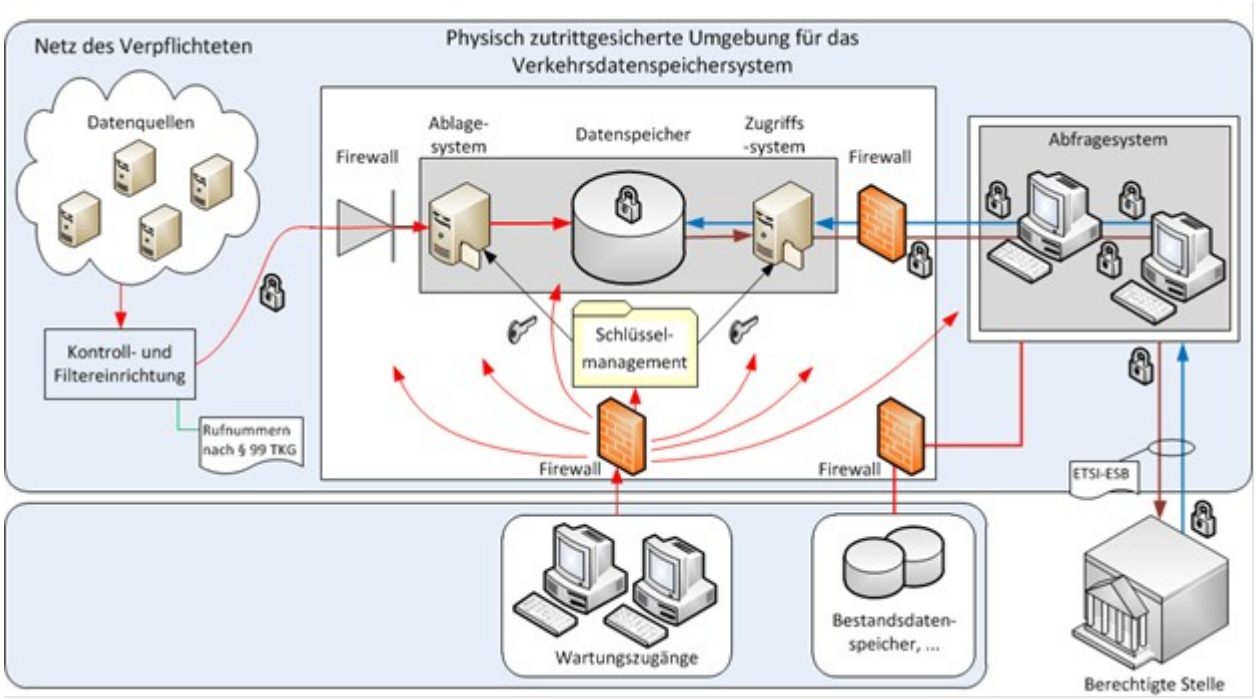


Abbildung: Umsetzungsbeispiel der Grundarchitektur (Quelle: Anforderungskatalog nach § 113f TKG)

Entsprechend dem ~~r Anforderungen im~~ Anforderungskatalog nach § 113f TKG gelten insbesondere folgende Anforderungen für die Übermittlung nach § 113c Abs. 3 TKG:

3.2.1 Gewährleistung eines besonders hohen Standards der Datensicherheit

Alle Komponenten des Übermittlungsverfahrens ETSI-ESB und E-Mail-ESB, beginnend vom Abfragesystem bis zum Übergabepunkt der verschlüsselten Übertragung (eigener Internetanschluss) an die berechtigte Stelle, müssen die Anforderungen nach IT-Grundschutz des BSI mit dem Schutzbedarf „hoch“ (siehe IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2) erfüllen.

3.2.2 Einsatz besonders sicherer Verschlüsselungsverfahren, Pufferung in den Komponenten des Übermittlungsverfahrens und Löschung der Verkehrsdaten im Abfragesystem

Die Verkehrsdaten müssen bei der Übermittlung mit einem geeigneten Verfahren verschlüsselt werden. Hierzu enthalten die nachfolgenden Beschreibungen der beiden Übermittlungsverfahren entsprechende Anforderungen.
Andere, als die dort genannten Verschlüsselungsverfahren dürfen nicht eingesetzt werden.

Zur Beauskunftung von Verkehrsdaten nach § 113b TKG ist nach demn ~~Anforderungen des~~ Anforderungskatalogs nach § 113f TKG vorgesehen, dass die Entschlüsselung d~~ies~~er Verkehrsdaten im Zugriffssystem erfolgen sollte. ~~Danach können die Abfrageergebnisse im Zugriffssystem entweder unverschlüsselt im flüchtigen Speicher (RAM) oder verschlüsselt im persistenten Speicher zwischengespeichert werden.~~ Zur Übermittlung der Abfrageergebnisse durch das Abfragesystem als Teil des Übermittlungsverfahrens können diese dort ~~ebenfalls~~ unverschlüsselt im RAM oder verschlüsselt im persistenten Speicher zwischengepuffert werden, wobei die verwendeten Schlüssel regelmäßig erneuert werden müssen.

Wenn das Abfragesystem sowie das Übermittlungsverfahren für weitere Auskunftserteilungen nach obigem Abschnitt 1 verwendet wird, muss sichergestellt sein, dass die Anbindung von hierfür erforderlichen weiteren Systemen über eine Firewall gesichert ist. Die Ausführungen zur Konfiguration der Firewall sowie zu den Log-Dateien gelten entsprechend dem Absatz 5.2.4 des Anforderungskatalogs nach § 113f TKG.

Die bei der Verarbeitung von Suchanfragen im Abfragesystem und im Übermittlungsverfahren anfallenden Klardaten (entschlüsselte Verkehrsdaten und andere temporäre Daten) sind direkt nach Übermittlung aus dem RAM zu löschen. Außerdem muss eine ungesicherte Auslagerung (Swap) von sensitiven Daten aus dem RAM verhindert werden. Zudem sind die Anforderungen nach Abschnitt 5.2.5 des Anforderungskatalogs nach § 113f TKG zu beachten.

3.2.3 Umsetzung des Vier-Augen-Prinzips bei Zugriff und Übermittlung der Verkehrsdaten

Um die Auskunftsersuchen der berechtigten Stellen durch besonders ermächtigte Mitarbeiter des Verpflichteten bearbeiten zu können, muss im Vier-Augen-Prinzip ein kontrollierter Zugriff über das Abfragesystem erfolgen. Die besonders ermächtigten Personen müssen sich hierzu mit individuellen Benutzerkennungen am Abfragesystem authentisieren. Die diesbezüglichen Protokollierungsvorschriften der TKÜV-Neu sind hierbei zu beachten.

Abhängig vom eingesetzten Übermittlungsverfahren muss das Abfragesystem so gestaltet werden, dass die beiden besonders ermächtigten Personen die folgenden Prüfungen vornehmen können:

a) Übermittlungsverfahren ETSI-ESB

Bei Nutzung der ETSI-ESB werden Anordnung und jeweilige Abfrageparameter durch die berechtigte Stelle übermittelt. Die beiden für den Zugriff besonders ermächtigten Personen prüfen in getrennten und unabhängigen Schritten die Übereinstimmung der in einer richterlichen bzw. staatsanwaltlichen Anordnung oder der in einem behördlichen Auskunftsersuchen enthaltenen Abfrageparameter mit den für den Zugriff bereitgestellten Abfrageparametern.

Im Abfragesystem ist hierbei sicherzustellen, dass die durch die berechtigte Stelle vorgegebenen Abfrageparameter durch die Prüfung bei dem Verpflichteten nicht geändert werden können. Bei etwaigen Fehlern oder Unklarheiten muss eine Rückmeldung an die berechtigte Stelle nach Abschnitt „Behandlung von Fehlern“

erfolgen. Liegt ein Fehler seitens der bS vor, muss der Prozess neu angestoßen werden (eine Korrektur durch den Verpflichteten beispielsweise nach telefonischer Absprache ist unzulässig).

b) Übermittlungsverfahren E-Mail-ESB

Bei Nutzung der E-Mail-ESB werden neben der Anordnung und ggf. weiteren Erläuterungen keine ~~weiteren~~ vordefinierten Abfrageparameter durch die berechtigte Stelle übermittelt. Die Abfrageparameter zum Zugriff auf die Verkehrsdaten müssen in einem ersten Schritt durch die erste der beiden hierfür besonders ermächtigten Personen festgelegt werden.

Die erste Person stellt die Abfrageparameter entsprechend der richterlichen Anordnung oder dem behördlichen Auskunftsersuchen im Abfragesystem ein.

Die zweite Person prüft in einem getrennten und unabhängigen weiteren Schritt die Übereinstimmung der in der richterlichen Anordnung oder der in einem behördlichen Auskunftsersuchen enthaltenen Abfrageparameter mit den für den Zugriff bereitgestellten Abfrageparametern.

Bei positivem Prüfergebnis initiiert die zweite Person den Zugriff auf die Verkehrsdaten und veranlasst gleichermaßen die Übermittlung des Abfrageergebnisses an die berechtigte Stelle. Bei negativem Prüfergebnis muss die erste Person die Abfrageparameter korrigieren; die zweite Person muss den Vorgang vor dem Zugriff erneut prüfen.

3.2.4 Physische Absicherung der Übermittlungsverfahren

Die Abfragesysteme sowie die sonstigen Einrichtungen des Übermittlungsverfahrens müssen physisch gegen den Zugriff durch nicht besonders ermächtigte Personen geschützt werden.

~~2.~~

Anlage A Übermittlungsverfahren ETSI-ESB

Diese Anlage beschreibt die nationalen Anforderungen an das Übermittlungsverfahren ETSI-ESB auf der Grundlage der ETSI-Spezifikation TS 102 657.

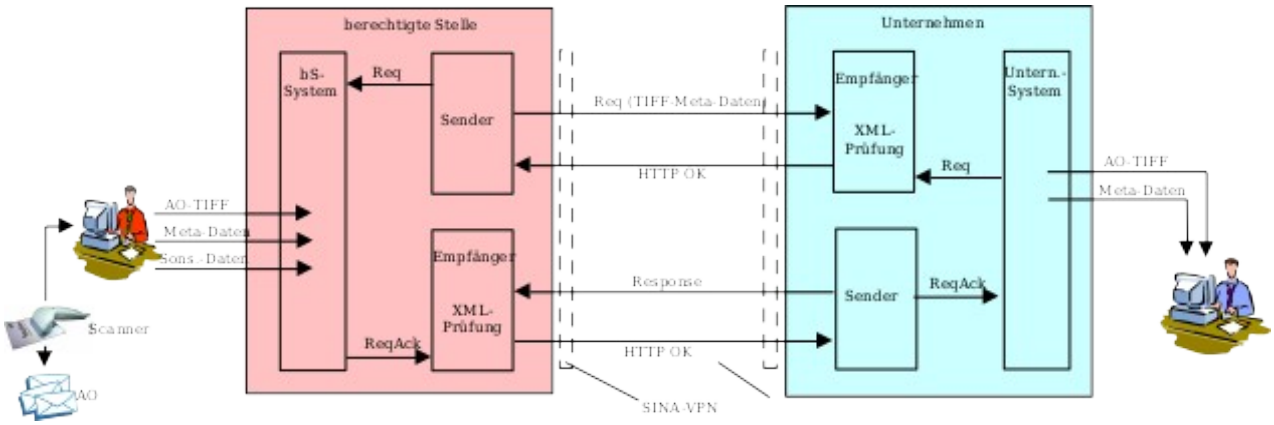
1.1 Grundsätzliche Verfahrensbeschreibung

Grundsätzlich richtet sich das Verfahren nach den Mechanismen, die in der ETSI-Spezifikation TS 102 657 beschrieben sind. Da diese Spezifikation weitere, national zu definierende technische Detaillierungen erfordert, sowie in Deutschland vorgegebene Anforderungen (wie z.B. die Anordnungspflicht) nicht kennt, bedarf es ergänzender Festlegungen, die über die Optionsauswahl zur Spezifikation hinausgehen.

Der grundsätzliche Übermittlungsmechanismus bedingt seitens der berechtigten Stellen sowie der verpflichteten Unternehmen je einen Empfänger und einen Sender, mittels derer initial eine Request-Nachricht von der berechtigten Stelle zum Unternehmen und daraufhin in einer eigenständigen Response-Nachricht die abgefragten Daten übermittelt werden.

Die Vorgänge werden i.d.R. durch die elektronische Übermittlung der Anordnung (AO) in einem *warrant-request* eingeleitet, dem dann eine oder mehrere eigentliche Abfragen in separaten *data-requests* folgen. Da die ETSI-Spezifikation nicht zwischen *warrant-* und *data-request* unterscheidet, beziehen sich diese Begriffe jeweils auf den dort beschriebenen uniformen Request.

Das Verfahren ist nachfolgend anhand eines Auskunftersuchens und der zugehörigen Auskunft über Verkehrsdaten ~~nach § 100g Abs. 1 StPO~~ für verschiedene Kennungen inkl. unterschiedlicher Zeiträume dargestellt:



1. Zur Administrierung der Anfrage bei der berechtigten Stelle gehört die Eingabe aller für den *warrant-request* notwendigen Metadaten sowie die elektronische Kopie der Anordnung. Die Metadaten enthalten die Informationen der Anordnung zu den verschiedenen Kennungen und Zeiträumen zur eigentlichen elektronischen Weiterverarbeitung. Beziehen sich die Metadaten auf mehrere abzufragende Kennungen, sind diese mit einer *targetNumber* als laufende Nummer versehen. Zudem können sonstige, nicht zu versendende Daten (z.B. Aktenzeichen, Beauskunftungsfrequenz) administriert werden. Der *warrant-request* wird automatisch durch eine individuelle *request-Number* (z.B. 4711) gekennzeichnet,
2. Nach Empfang des *warrant-requests* und nach automatischer Überprüfung der Lesbarkeit sowie der Vollständigkeit erfolgt die manuelle Prüfung und Freigabe der in den Rahmen der Anordnung fallenden Metadaten zur Auskunfterteilung durch den oder die Personen, die dazu von dem Verpflichteten besonders ~~bevoll~~ermächtigt wurden ~~en-~~

Bearbeiter des Unternehmens (Operator). Dabei darf die Freigabe nur erfolgen, wenn die Metadaten mit den Angaben in der Anordnung übereinstimmen.

Die Freigabe erfolgt unter Bezug auf die jeweilige Anordnung für alle dort genannten Kennungen inkl. der Zeiträume; diese Freigabe ist durch die *request-Number* des *warrant-requests* (hier 4711) gekennzeichnet.
Für jede konkrete Anfrage zu Verkehrsdaten wird ein separater *data-request* nötig:

1. Aufgrund der Einstellungen im bS-System wird ein separater *data-request* manuell oder automatisch versendet, der die Abfrage zu einer konkreten Kennung sowie einem konkreten Zeitraum beinhaltet. Dieser *data-request* wird wiederum durch eine individuelle *requestNummer* (z.B. 4922) gekennzeichnet und enthält als Referenz zum *warrant-request* dessen *requestNumber* als *referencedRequestNummer* (hier 4711). Zusätzlich wird mit der *targetNumber* auf die laufende Nummer in den Metadaten des *warrant-requests* referenziert.

2. Nach Empfang des *data-requests* und nach automatischer Überprüfung der Lesbarkeit sowie der Vollständigkeit erfolgt der automatische Abgleich mit den durch die Freigabe hinterlegten Metadaten und der *targetNumber*. Sind die konkret abgefragte Kennung sowie der konkrete Zeitraum durch die Metadaten abgedeckt, erfolgt die automatisierte Beauskunftung.

Die Übermittlung der Daten, die aufgrund der der Abfrage zugrunde gelegten Kennung ermittelt wurden, erfolgt durch eine separate Response-Nachricht, die mit der *requestNummer* des *data-requests* (hier 4922) gekennzeichnet ist. Die Übermittlung der vom Unternehmen ausgehenden Nachricht erfolgt nach dem beschriebenen Prinzip, jedoch mit vertauschten Rollen.

1.2 Verfahrensbedingungen

- **Nutzung der ETSI-Definitionen sowie nationaler Ergänzungen**
  Für die Bereitstellung der elektronischen Anordnung sowie der Metadaten im *warrant-request* sowie den darauffolgenden *data-requests* wird die Nutzung einer nationalen XML-Definition *Natparas2* notwendig, die mittels des XML-Moduls der ETSI-Spezifikation übermittelt wird. Für die Beauskunftung von Verkehrsdaten durch das Unternehmen mittels der Response-Nachricht werden keine national ergänzenden Parameter benötigt.
  Für die weiteren Nutzungen (z.B. Bestandsdaten, Ortung) ist die Übermittlung der ergänzenden XML-Definition *Natparas3* für die Übermittlung der Antwortdaten mittels der Response-Nachricht notwendig.
- **Fehlende Übereinstimmung der Metadaten mit der Anordnung**
  Stimmen die Metadaten im *warrant-request* nicht mit den Angaben der Anordnung überein, können die betroffenen Daten dieses Teils des *warrant-requests* nicht zur Auskunfterteilung freigegeben werden. In diesen Fällen erfolgt eine Rückmeldung mit einer *ResponseIncomplete*-Nachricht nach Abschnitt 2.2.2.4, die eine automatisch auswertbare Liste (*TargetNumber*) der als ungültig gewerteten Kennungen enthält. Für die fehlerfreien Abfragen zu weiteren Kennungen muss bei Übereinstimmung mit der Anordnung die Freigabe erfolgen.

  Nach Klärung durch die bS muss der Vorgang in einem separaten *warrant-request* erneut vorgelegt werden, wenn das Erfordernis einer Auskunfterteilung für die fehlerhaften Einträge weiterhin besteht. Hierzu kann der neue *warrant-request* entweder
  - eine korrigierte Anordnung sowie die unveränderten Metadaten für die betroffene Kennung oder
  - die unveränderte Anordnung sowie die korrigierten Metadaten der betroffenen Kennungen
  enthalten.

  Sollten für Kennungen, die in der Anordnung benannt sind, keine Abfragen gestellt werden, sind hierfür keine Metadaten einzutragen (eine Fehlermeldung ist hierfür nicht

erforderlich).

Die Zurückweisung des gesamten *warrant-requests* ist nur in Fällen vorgesehen, in denen grundsätzliche Mängel bestehen bzw. vermutet werden (z.B. bei schlechter elektronischer Kopie der Anordnung oder komplett fehlenden oder fehlerhaften Metadaten). Auch hierzu muss die Rückmeldung mit einer *FailureResponse*-Nachricht nach Abschnitt 2.2.2.3 erfolgen.

- **Parallele Versendung von warrant- und data-request**
  Regelmäßig werden für einen *warrant-request* erste darauf bezogene *data-requests* gleichzeitig versendet. Das empfangende System der Unternehmen muss daher einen Mechanismus vorhalten, vorliegende *data-requests* dann unmittelbar zu bearbeiten, wenn der entsprechende *warrant-request* freigegeben wurde.

- **Getrennte Verfahren für die verschiedenen Nutzungen der Schnittstelle**
  ~~Um einen möglichst einfachen Prozessablauf des Abfrage-Systems zu ermöglichen, ist es nicht vorgesehen, in einem *warrant-request* Metadaten zu verschiedenen Nutzungen zu kombinieren. So sind etwa kombinierte , wie etwa die Abfragen von Verkehrsdaten nach § 1010g Abs 1 und nach § 100g Abs. 2 StPO, „normale“ Abfragen von Verkehrsdaten und von Verkehrsdatenabfragein Echtzeit sowie und eine kombinierte die Aktivierung einer von Überwachungsmaßnahme zur betreffenden Kennung nicht vorgesehen. Verschiedene Nutzungen erfordern verschiedene *warrant-requests*, auch wenn dabei die gleiche elektronische Anordnung verwendet wird und die gleiche Kennung betroffen ist.~~

  Um einen möglichst einfachen Prozessablauf des Abfrage-Systems zu ermöglichen, ist eine Kombination der unter „1. Grundsätzliches“ aufgeführten Anwendungsfälle nicht erlaubt. Verschiedene Nutzungen erfordern verschiedene warrant-requests, auch wenn dabei die gleiche elektronische Anordnung verwendet wird und die gleiche Kennung betroffen ist.

- **Mehrere Kennungen pro warrant-request, jeweils eine Kennung pro anschließender Abfrage bzw. Beauftragung**
  Jede eigentliche Abfrage bzw. Beauftragung (z.B. *data-request*, *activation-request* etc.) enthält genau eine konkret angegebene Kennung (eine Kennung kann neben den in Kapitel 4.1 in Teil A dieser TR TKÜV aufgeführten Arten auch aus mehreren Bestandteilen wie z.B. Name und Anschrift bestehen, sofern diese zur eindeutigen Bestimmung notwendig sind), die Meta-Anfragen im *warrant-request* können entsprechend den möglichen Mehrfachnennungen der Anordnung mehrere Kennungen beinhalten.

- **Besonderheiten bei Übermittlung von Anordnungen zur Umsetzung von Überwachungsmaßnahmen**
  Parallel zur Beauskunftung von Verkehrsdaten kann diese Schnittstelle zur Umsetzung von Überwachungsmaßnahmen nach Abschnitt 1.3.6 genutzt werden.

- **Nutzung einheitlicher Formate und Parameter**
  Wie für die Anforderungen nach Teil A der TR TKÜV bietet die ETSI-Spezifikation verschiedene Möglichkeiten zur Beauskunftung eines Datums (z.B. IP-Adresse im ASCII- oder Binär-Format). Soweit beim Unternehmen vorliegende Daten zur Beauskunftung erst in eines dieser Formate umgewandelt werden müssen, ist die in Abschnitt 2.2.3 gelistete Kodierung zu verwenden. Die berechtigten Stellen müssen die dort aufgeführten Kodierungen innerhalb ihrer requests verwenden. Darüber hinaus wird in Abschnitt 2.2.4 festgelegt, welche XML-Parameter genutzt werden, wenn die Struktur der ETSI-Spezifikation alternative Parameter ermöglicht (Normierung).

- **Nutzung neuerer Versionen der nationalen XSD und der ETSI-XSD**
  Neuere Versionen der nationalen XML-Module sowie der ETSI-XSD dürfen von den Verpflichteten frühestens sechs Monate nach deren Veröffentlichung eingesetzt

werden. Die Bundesnetzagentur kann bei dringendem Bedarf einem früheren Einsatz zustimmen. In der Übergangszeit erfolgt die Beauskunftung von in der Vorgängerversion noch nicht definierten ~~„neueren“~~ Daten mittels des Parameters <additionalInformation>. Die bSn müssen die von den einzelnen Verpflichteten genutzten Versionen unterstützen und verwenden.
Bei Versionskonflikten erfolgt eine Fehlermeldung nach Abschnitt 2.2.2.2, die die unterstützte Version enthält.

- **Abweichungen von den Vorgaben der ETSI-Spezifikation**
  Um den Verfahrensablauf zu vereinfachen und die besonderen Anforderungen in Deutschland zu erfüllen, gelten folgende Abweichungen von dem in der ETSI-Spezifikation vorgesehenen Mechanismus:

  1. Um Requests zu den Verkehrsdaten sämtlicher genutzter Dienste (z.B. Telefondienst, Internetzugangsdienst) einer Kennung zu ermöglichen, gilt entgegen Kapitel 6.2.1 der ETSI-Spezifikation, dass die Response-Message die Verkehrsdaten verschiedener Dienste enthalten kann.
  2. Um für den *data-request* ein einheitliches Schema zu verwenden, wird grundsätzlich der Telefoniebereich der ETSI-Spezifikation genutzt. Demnach wird beispielsweise für einen request zu den Verkehrsdaten sämtlicher Vorgänge einer E-Mail Adresse die E-Mail Adresse im Feld emailAddress von partyInformation des Telefoniebereiches eingetragen. Nach Abschnitt 2.2.3.4 ist zudem eine kombinierte Beauskunftung möglich. Dabei wird durch eine Erweiterung des Feldes „nationalTelephonyServiceUsage“ erreicht, dass über die Beauskunftung für den Telefondienst auch der Internetzugangsdienst beauskunftet werden kann.

- **Anforderungen an das einzusetzende Verschlüsselungsverfahren**
  Bei Einsatz des Übermittlungsverfahrens ETSI-ESB sind ausschließlich die in Anlage A.1 dieses Teils der TR TKÜV sowie die in der aktuellen Policy (Anlage X.3) vorgegebenen Systeme mit den dort beschriebenen Verschlüsselungsverfahren vorgesehen.
  Die Systeme verfügen über keine Speicher für die zu übertragenen Daten. Die automatisierte Protokollierung der Übertragungen enthalten keine Hinweise auf die Art der übertragenen Daten.

1.3 Besonderheiten der verschiedenen Verwendungsmöglichkeiten

Nachfolgend werden Besonderheiten der verschiedenen Verwendungsmöglichkeiten beschrieben.

1.3.1 Beauskunftung von Verkehrsdaten nach § 96 und § 113b TKG (optional)

Zur Beauskunftung von Verkehrsdaten ist vor den automatisch zu verarbeitenden *data-requests* die Übermittlung und Überprüfung eines *warrant-requests* notwendig. Die Übermittlung der Anordnung mittels dieser Schnittstelle ist zwingend vorgeschrieben. Durch die unabhängige Versendung der *data-requests* können die bSn die Häufigkeit und den abgefragten Zeitraum aufgrund der Informationen der verpflichteten Unternehmen zu den Speicherfristen der von ihnen vorgehaltenen Verkehrsdaten individuell gestalten. Vorgaben einer festen Beauskunftungsfrequenz für in die Zukunft gerichtete Abfragen ~~sowie zur automatischen Nachlieferung von zum Zeitpunkt der Abfrage noch nicht vorliegenden Verkehrsdaten~~ sind daher nicht vorgesehen.

Gemäß § 113c Abs. 3 Satz 2 TKG ist eine Kennzeichnung der zu beauskunfte~~t~~nden Verkehrsdaten nach § ~~-~~96 und § 113b TKG zwingend vorgesehen. Für die Beauskunftung größerer Datenmengen sieht die ETSI-Spezifikation nach Abschnitt 5.1.7 die Übermittlung in verschiedenen Teilen vor. ~~Darüber hinaus kann die Lieferung der zu beauskunftenden Verkehrsdaten auf einem Datenträger mit der bS abgesprochen werden.~~

1.3.1.1 Automatische Nachlieferungen von Late-records nach Festlegung der berechtigten Stelle

Die bSn können mittels eines besonderen *data-requests* die Beauskunftung von verspäteten Verkehrsdaten (Late-records) festlegen, die erst nach einer Wartezeit und nach dem Ablauf des abgefragten Zeitraums im *warrant-request* zur Verfügung stehen. Die mit der Bundesnetzagentur abzustimmende Wartezeit muss so bemessen sein, dass Late-records regelmäßig vollständig erfasst werden. Die Beauskunftung erfolgt in einer regulären *response-message* und enthält alle zu diesem Zeitpunkt für den gesamten Zeitraum gespeicherten Verkehrsdaten. Diese Festlegung kann durch die bSn mittels einesr ~~weiteren *data-requests* (~~Cancel-Message~~)~~ zurückgezogen werden.

Sollen Late-records für einen bestimmten Teilzeitraum vor Ablauf des gesamten Zeitraums beauskunftet werden, können diese durch einen zweiten *data-requests* abgefragt werden. Hierzu können beispielsweise *data-requests* für einen zweiten Teilzeitraum überlappend den ersten Teilzeitraum abfragen.

1.3.1.2 Selektive Beauskunftung von Verkehrsdaten~~, Zielwahlsuche~~

Die Beauskunftung von Verkehrsdaten muss grundsätzlich in selektiver Form erfolgen können (§ 101a Abs. 1 Satz 1 Nr. 1 StPO). Hierfür müssen mithilfe des XML-Elements *<requestedData>* der ETSI-XSD die zu beauskunftenden Parameter in XPATH-Notation angegeben werden. Im Gegensatz zur nicht-selektiven Beauskunftung werden dadurch ausschließlich die durch die bS angeforderten Parameter beantwortet. Bei Nutzung dieses XML-Elements sind im Gegensatz zu dem Verfahren nach Abschnitt 1.3.1 nur die selektiv angefragten Daten zu übermitteln.

Falls das ausgewählte Element „child nodes“ aufweist, gilt der gesamte darunter liegende XML-Unterbaum als ausgewählt. Es sind ausschließlich absolute Pfadangaben zulässig, d.h. Jokerzeichen oder sonstige Suchoperatoren oder logische Verknüpfungen wie bspw. UND, ODER, XODER dürfen nicht verwendet werden.

1.3.1.3 Selektive Beauskunftung von Verkehrsdaten bei Zielwahlsuche

In Ergänzung des vorherigen Abschnittes gilt, dass zur Beauskunftung von Verkehrsdaten, die zu einer bestimmten Zieladresse oder von einer bekannten Rufnummer (Ursprungsadresse) zu unbekannten Zieladressen hergestellt wurden (Zielwahlsuche), ~~sind~~ folgende Parameter neben der Kennzeichnung in den Natparas2 der ETSI-XSD zu belegen sind:

- Zielwahlsuche zu einer bekannten Zieladresse:

  TelephonyServiceUsage/partyInformation/partyNumber: Zielrufnummer
  ~~/calledPartyNumber~~ (E.164 Format):
  Angabe der bekannten Zieladresse
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Tag Nummer 1, „terminating-Party“

- Zielwahlsuche von einer bekannten Rufnummer (Ursprungsadresse):

  TelephonyServiceUsage/partyInformation/partyNumber:
  Ursprungsadresse~~/callingPartyNumber~~ (E.164 Format):
  Angabe der bekannten Ursprungsadresse
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Tag Nummer 1, „originating-Party“.

1.3.2 Beauskunftung von Verkehrsdaten ~~nach § 96 TKG~~ in Echtzeit ~~z.B. nach § 100g Abs. 1 Satz 3 StPO~~ (optional)

In Ergänzung zu den Ausführungen nach Abschnitt 1.3.1 gilt:

Um die Bedingungen der Echtzeitanforderung zu erfüllen, ~~müssen~~ können diejenigen verpflichteten Unternehmen, die die ~~eine~~ Schnittstelle zur Übermittlung der zu überwachenden Telekommunikation nach Teil A vorhalten, derartige Auskunftersuchen durch

die Administrierung einer IRIOnly-Maßnahme (Bereitstellung der Daten nach § 7 TKÜV) umsetzen. Dazu muss die Überwachungstechnik so angepasst werden, dass

1. die übermittelten Daten keine Nachrichteninhalte (z.B. SMS) enthalten,
2. ~~im Mobilfunkbereich~~ Standortdaten auch für lediglich empfangsbereite Mobilfunk-Endgeräte erhoben und übermittelt werden und
3. die Übermittlung der Standortdaten nach Nummer 2 derart eingeschränkt werden kann, dass sie für die bSn nur nach Maßgabe der jeweils geltenden Vorschriften (z.B. § 100g Abs. 1 StPO) erfolgt.

Alternative Vorkehrungen ~~Darüber hinaus müssen~~ zur Umsetzung derartiger Auskunftersuchen ~~keine zusätzlichen Implementierungen zur Beauskunftung von Verkehrsdaten vorgesehen werden~~müssen gleichwertig und in Abstimmung mit der Bundesnetzagentur gestaltet werden.

Kann das Unternehmen derartige Auskunftersuchen, beispielsweise in Fällen von temporären Kapazitätsengpässen bei der Administrierung von Überwachungsmaßnahmen nicht umsetzen, kann die Beauskunftung nach Zustimmung der bS durch ein Verfahren nach Abschnitt 1.3.1 umgesetzt werden.

Für die zugehörigen Nachrichten (warrantRequest und dataRequest) ist nach Abschnitt 2.2.1 der Port für die Übermittlung der Anordnung zur Überwachung der Telekommunikation zu verwenden; eine Unterscheidung der beiden Nutzungen erfolgt durch die angegebene Rechtsgrundlage.

1.3.3 Beauskunftung zur Struktur von Funkzellen (optional)

Die beschriebene Schnittstelle sowie das in Abschnitt 1.3.1 beschriebene Verfahren kann optional zur Beauskunftung zur Struktur von Funkzellen genutzt werden.

1.3.4 Beauskunftung von Bestandsdaten gemäß § 113 Abs. 5 Satz 2 TKG

Der Einsatz der beschriebenen Schnittstelle sowie des in Abschnitt 1.3.1 beschriebenen Verfahrens ist gemäß § 113 Abs. 5 Satz 2 TKG zur Beauskunftung von Bestandsdaten für alle TK-Anbieter mit mehr als 100.000 Teilnehmern verpflichtend.

Mit der Übermittlung des warrantRequests und des dataRequests ist die Bestandsdatenanfrage zugestellt. Der warrantRequest hat die formalen Anforderungen des § 113 Abs. 2 TKG (u.a. an die Textform und unter Angabe der gesetzlichen Grundlage) zu erfüllen und beinhaltet jeweils ein *WarrentTarget* (kein Mehrfachbezug möglich). Er enthält zudem die optionale Liste zur selektiven Abfrage. Zur Umsetzung der Textform stehen wahlweise das XML-Element <warrantTIFF> oder <warrantTextform> zur Verfügung.

Der dataRequest ist mit dem warrantRequest oder unmittelbar danach zu verschicken. Der dataRequests weist keine inhaltlichen Abweichungen (z.B. keine Unmengen) zum warrantRequest auf. Für die Fälle, in denen die ETSI-XSD keine passenden Felder für die Abfragedaten vorsieht, enthält die nationale Ergänzung die hierzu notwendigen Felder. Folgt auf den warrantRequest innerhalb einer Stunde kein dataRequest (bzw. umgekehrt), wird der abgeschlossen und für den warrentRequest (bzw. *dataRequest*) eine *FailureResponse* versendet.

Die Bearbeitung der Anfrage beginnt mit der formalen Prüfung des warrantRequests durch eine verantwortliche Fachkraft, sobald auch der dataRequest vorliegt. Eine automatisierte Prüfung ist rechtlich nicht zulässig. Die Beauskunftung erfolgt nach Eingang des dataRequests.

1.3.4.1 Sselektive Beauskunftung von Bestandsdaten

Die Beauskunftung von Bestandsdaten muss grundsätzlich auch in selektiver Form erfolgen können. Hierfür müssen mithilfe des XML-Elements *<requestedData>* der ETSI-XSD die zu beauskunftenden Parameter in XPATH-Notation angegeben werden. Im Gegensatz zur nicht-selektiven Beauskunftung werden dadurch ausschließlich die durch die bS angeforderten Parameter beantwortet. Bei Nutzung dieses XML-Elements sind im Gegensatz zu dem Verfahren nach Abschnitt 1.3.4 nur die selektiv angefragten Daten zu übermitteln.

Falls das ausgewählte Element „child nodes“ aufweist, gilt der gesamte darunter liegende XML-Unterbaum als ausgewählt. Es sind ausschließlich absolute Pfadangaben zulässig, d.h. Jokerzeichen oder sonstige Suchoperatoren oder logische Verknüpfungen wie bspw. UND, ODER, XODER dürfen nicht verwendet werden. Umfasst die Anfrage das Datenfeld PUK der ETSI-XSD, so ist damit ebenfalls die PIN mit angefragt, welche bei Vorliegen vom Verpflichteten im entsprechenden Feld der *NatParas3* zu berichten ist.

1.3.5 Beauskunftung zur Standortfeststellung von mobilen Endgeräten (optional)

Zur Beauskunftung zur Standortfeststellung von mobilen Endgeräten, beispielsweise zur Gefahrenabwehr nach Landesrecht oder im Zusammenhang mit einer Überwachungsmaßnahme, kann optional die beschriebene Schnittstelle nach dem im Abschnitt 1.3.1 beschriebenen Verfahren genutzt werden.

Durch die Anforderungen der ~~möglichst~~ sofortigen Verfügbarkeit der Ergebnisse solcher Abfragen an wechselnden Orten (z.B. Einsatzstellen bei Vermisstensuchen) kann ein solches elektronisches Verfahren, welches von örtlich festgelegten Abfragestellen ausgeht, nicht immer gerecht werden. Daher ist es regelmäßig erforderlich, parallel ein „manuelles“ Verfahren, beispielsweise mittels Telefon ~~und Telefax~~, zu unterhalten.

1.3.6 Übermittlung der Anordnung sowie weitere Maßnahmen zur Überwachung der Telekommunikation (optional)

Die Nutzung dieser Schnittstelle erfüllt die Bedingungen des § 12 Abs. 2 Satz 1 TKÜV nach auf gesichertem elektronsichen Weg übermittelten Kopie der Anordnung. Das Vorlegen des Originals oder einer beglaubigten Abschrift der Anordnung ist in diesen Fällen nicht erforderlich.

Wie zum Verfahren der Beauskunftung von Verkehrsdaten ist zur Umsetzung von Überwachungsmaßnahmen zunächst die Freigabe aufgrund eines *warrant-request* notwendig; zur Aktivierung bzw. Deaktivierung der Maßnahmen wird ein separater *activation-* oder *deactivation-request* versendet. Verschiedene betroffene Kennungen werden durch eine targetNumber als laufende Nummer gekennzeichnet.

Änderungen einer aktiven Maßnahme, die keine weitere Anordnung voraussetzen, werden durch einen *modify-request* umgesetzt.

Änderungen einer aktiven Maßnahme, die eine weitere Anordnung voraussetzen, werden durch einen zweiten *warrant-request* eingeleitet und einen zweiten *activation-request* aktiviert. Metadaten von Einzelmaßnahmen bzw. Kennungen des ersten *warrant-requests*, die von der Änderung nicht betroffen sind, dürfen im zweiten *warrant-request* zur Einleitung der Änderung nicht enthalten sein.

Wie zum Verfahren der Beauskunftung von Verkehrsdaten können *activation-*, *modification-modify-* und *renewal request* nach Gegenprüfung mit den Metadaten des *warrant-requests* automatisiert bearbeitet werden.

Bei der Nutzung dieser Möglichkeit muss die Pflicht zur Protokollierung nach § 16 TKÜV beachtet werden, nach dem jegliche Anwendung der Überwachungseinrichtung erfasst werden muss und damit unabhängig davon gilt, ob die Anwendung manuell oder automatisiert erfolgt.

Die nachfolgenden Darstellungen zeigen den Ablauf der Durchführung einer Überwachungsmaßnahme mit zwei betroffenen Kennungen (Abbildung A) sowie der Verlängerung einer Maßnahme (Abbildung B):

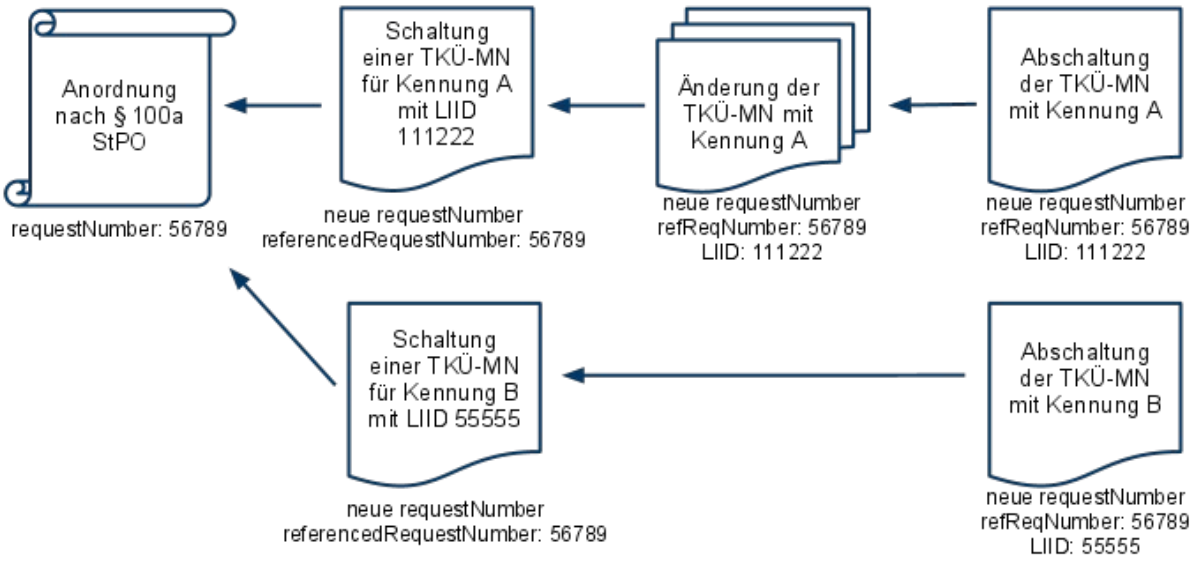


Abbildung A: Durchführung einer Überwachungsmaßnahme für die Kennungen A und B

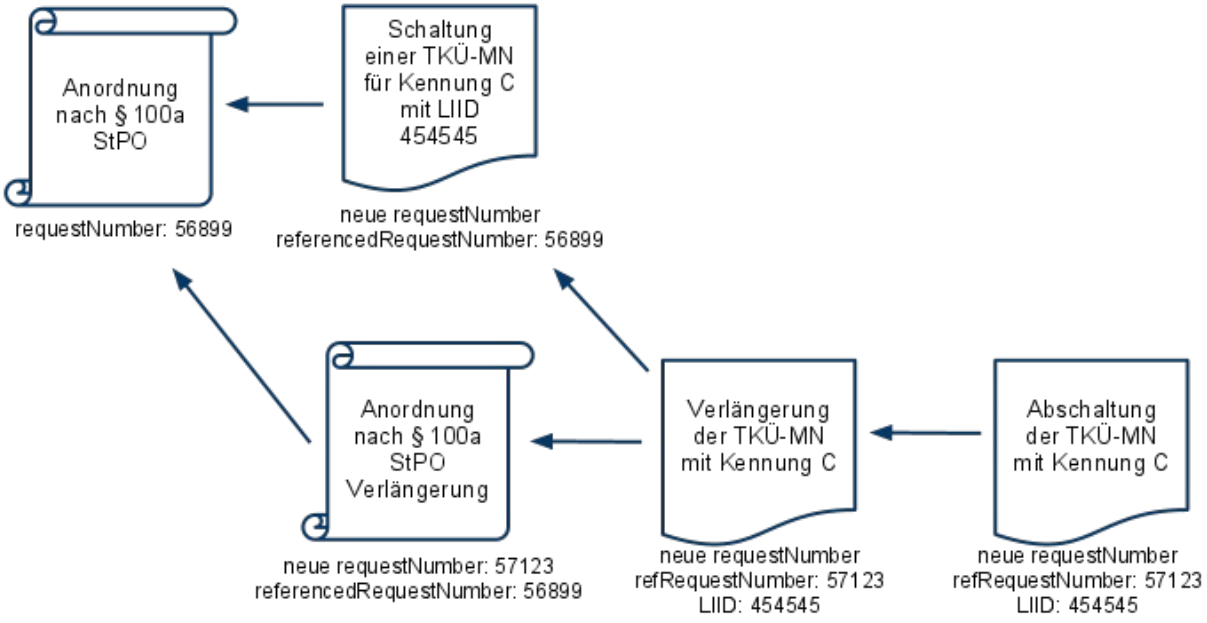


Abbildung B: Durchführung und Verlängerung einer Überwachungsmaßnahme für die Kennung C

1.3.7 Übermittlung von Daten zum Rechnungsabgleich im Vorfeld der Entschädigung nach § 23 Absatz 1 JVEG (optional)

Siehe Abschnitt 4.

1.4 Elektronisch gesicherte Übermittlung der Anordnung

Für ein gemäß Teil B der TR TKÜV beschriebenes Verfahren der gesicherten elektronischen Übermittlung der Anordnung, mittels Nutzung des SINA-VPN nach Anlage A-2, **entfällt** ~~nach Maßgabe des § 12 Abs. 2 Satz 1 TKÜV~~ die Notwendigkeit der nachträglich postalischen Übermittlung des Originals bzw. einer beglaubigten Abschrift der Anordnung.

Durch die Vorgabe der Nutzung des SINA-VPN ist die Sicherheit der elektronischen Übermittlung im Sinne der Anforderung des § 12 Abs. 2 TKÜV gegeben.

Bei der Anwendung dieses Verfahrens und der damit möglichen Vorbelegung von Administrierungsoberflächen muss jedoch sichergestellt sein, dass eine automatisierte Umsetzung der Anordnung nicht vorgenommen werden kann. Vielmehr ist in jedem Einzelfall eine „manuelle Prüfung“ vorzunehmen. Erst nach dieser manuellen Prüfung und der daraufhin erfolgten Freigabe im System kann die Maßnahme manuell bzw. durch einen weiteren request automatisiert aktiviert werden.

Format der Anordnung

Die Kopie der Anordnung ist zur Übermittlung in das Multipage TIFF-Format (CCITT Faxgruppe 4) umzuwandeln. Die maximale Dateigröße beträgt 5 MB. Enthält eine Folgeanordnung nicht alle notwendigen Daten (z.B. Rechtsgrundlage, Kennung, Zeitraum), muss sie zusammen mit der Ursprungsanordnung in einer Datei übermittelt werden. Bei zuvor per Telefax übermittelten Anordnungen muss auf eine Mindestqualität geachtet werden. Diese muss **mindestens** der hohen Auflösung (203 oder 204 dpi horizontal; 196 dpi vertikal) gebräuchlicher Telefaxgeräte entsprechen (dies entspricht üblicherweise der Einstellung „fein“).

2 Festlegungen für den Übergabepunkt nach der ETSI-Spezifikation TS 102 657

Dieser Abschnitt beschreibt die Bedingungen für den Übergabepunkt nach der ETSI-Spezifikation TS 102 657 [31].

Die Anlage beinhaltet die Entscheidung über die in den Spezifikationen enthaltenen Optionen und die Festlegung ergänzender technischer Anforderungen. Mittels des in der ETSI-Spezifikation beschriebenen XML-Moduls wird jeweils eine Abfrage übermittelt; eine Paketierung mehrerer Abfragen ist nicht vorgesehen.

Neben den Anforderungen dieses Teils sind zudem folgende Anlagen des Teils X der TR TKÜV gültig:

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module

2.1 Optionsauswahl zur ETSI TS 102 657

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 657 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 657	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.1	**Reference model** Unterschiedliche *Authorized Organizations* für HI-A und HI-B sind nicht vorgesehen.	Siehe hierzu die Festlegungen in dieser Tabelle zu Kapitel 5.4
4.5	**Model used for the RDHI** Als Übermittlungsmechanismus wird XML/HTTP genutzt.	Siehe hierzu die Festlegungen in dieser Tabelle zu Kapitel 7 bzw. im Anschluss an diese Tabelle.
5.1.2	**Message flow modes** Grundsätzlich ist nur die Variante *General situation* nach Kapitel 5.2 vorgesehen.	Die angefragten Daten werden vom Verpflichteten unverzüglich an die berechtigte Stelle übermittelt (Push-Verfahren).
5.1.5	**Errors and failure situations** Fehler nach 5.1.5.2 werden mit einer qualifizierten Fehlermeldung an die bS gemeldet. Bei formal fehlerhaften Übertragungen (Fehler nach 5.1.5.3) wird die Annahme vom Empfänger verweigert.	Siehe hierzu die Festlegungen im Abschnitt 2.2.2 dieser TR TKÜV im Anschluss an diese Tabelle.
5.1.7	**Delivery of results** Die Option *single shot delivery* muss, die Option *multi-part delivery* kann implementiert werden.	Bei der Option *single shot delivery* ergibt sich zu jeder Abfrage genau eine Antwort. In Fällen von in die Zukunft gerichteten Anordnungen zur Erteilung von Auskünften über Verkehrsdaten sind die der jeweiligen

Abschnitt TS 102 657	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
		Anordnung zuzuordnenden einzelnen Abfragen (requests) unter Berücksichtigung der Zeiträume, in denen die betreffenden Daten bei den Unternehmen gespeichert sind, von den berechtigten Stellen an die Unternehmen zu versenden. Die Option *multi-part delivery* ermöglicht die Aufteilung einer Beauskunftung in mehrere Teilmengen, wenn die zu übermittelnden Verkehrsdaten umfänglich sind. Wenn diese Option implementiert wird, muss der Parameter ResponseNumber verwendet werden. Die Nutzung sowie die genaue Ausgestaltung der Verwendung muss im Konzept beschrieben werden. Für beide Optionen gelten zusätzlich folgende Hinweise: 1. Die grundlegende Verpflichtung der Telekommunikationsunternehmen nach § 96 TKG, nicht benötigte Verkehrsdaten unverzüglich nach Verbindungsende zu löschen, bleibt unberührt, 2. Aus der Ausgestaltung des technischen Verfahrens erwächst weder die Pflicht noch die Berechtigung, Verkehrsdaten über den durch § 96 TKG gesteckten Rahmen zu speichern.
5.5	**HI-A and HI-B addressing** Das Feld *deliveryPointHIB* wird nicht verwendet.	Unterschiedliche IP-Adressen für eine *Authorized Organization* sind innerhalb einer Anfrage und der zugehörigen Antwort nicht zulässig, d.h. Quell-IP-Adresse für HI-A und Ziel-IP-Adresse für HI-B müssen identisch sein.
6.1.2	**RequestID field specification** Die benötigte Kennung *Authorized Organization Code* der berechtigten Stelle wird von der Bundesnetzagentur vorgegeben. In Fällen, in denen die berechtigte Stelle für einen gesendeten request keine ACK-Message erhält, kann sie den gleichen request inkl. der gleichen *RequestNumber* erneut senden. Das Verfahren ist im Abschnitt 2.2.2.5 dieser TR TKÜV beschrieben.	Der Authorized Organization Code der berechtigten Stelle entspricht der bS-ID, die im Rahmen eindeutiger Referenznummern für TKÜ-Maßnahmen vergeben wird (siehe hierzu Anlage X.2 der TR TKÜV). Die Erkennung doppelter *RequestNumbers* durch den Verpflichteten ist auf die ihm noch vorliegenden Daten beschränkt. Sie bedingt keine Abweichung datenschutzrechtlicher Löschungen.
6.1.3	**CSP Identifiers** Die benötigten Kennungen CSP ID und Third Party CSP ID der Verpflichteten werden von der Bundesnetzagentur vorgegeben.	Die CSP ID der Verpflichteten entspricht der Operator-ID, die im Rahmen der Verpflichtung nach Teil A und / oder Teil B dieser TR TKÜV erteilt wurden.
6.1.4	**Timestamp** Es gelten die Einschränkungen nach Abschnitt 2.2.3.1 dieser TR TKÜV	

Abschnitt TS 102 657	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
6.3.1 6.3.2	**Information contained within a request** Kennungen sind mit equals anzufragen. Die Range-Parameter *lessThanOrEqualTo* und *greaterThanOrEqualTo* sind nur für die Zeitangaben zu verwenden.	Nicht zu verwenden sind: *notEqualTo, lessThan, greaterThan, startsWith, endsWith, isAMemberOf*
6.3.3	**Additional information in requests** Alle Requests haben die gleiche Priorität. Der MaxHits Parameter ist nicht zu verwenden.	
6.4	**Error messages** Fehlermeldungen müssen aussagekräftig gestaltet werden. Wenn bspw. Versionskonflikte entstehen, müssen die Fehlermeldungen zumindest die erwartete Version beinhalten.	
7	**Data exchange techniques** Als Übermittlungsmechanismus wird XML/HTTP genutzt. Die Übertragung erfolgt in einem VPN gemäß Anlage A-2 über das öffentliche Internet.	Siehe hierzu die Festlegungen im Abschnitt 2.2 dieser TR TKÜV bzw. im Anschluss an diese Tabelle.
7.2	**HTTP data exchange** Die Option *Mutual client/server* ist zu verwenden.	Siehe hierzu die Festlegungen im Anschluss an diese Tabelle.
7.2.3	**Mutual client/server** URI ist für HI-A und HI-B einheitlich /etsi	Der Host-Header wird nicht benötigt.
8	**Security Measures** Es gelten die Anforderungen nach Anlage A-2.	
Annex A	**Data fields** Die Anlage beschreibt die genutzten Datenfelder und die Festlegungen innerhalb einer ASN.1-Definition. Die zu nutzende XML-Definition ist zusammen mit der ETSI-Spezifikation über die Webseite von ETSI zu beziehen.	Beispiele gängiger Abfragen und die grundsätzlich erwarteten Ergebnisse können bei der Bundesnetzagentur abgefragt werden.

2.2 Ergänzende technische Anforderungen zur Schnittstellenbeschreibung der ETSI TS 102 657

Der in der ETSI-Spezifikation beschriebene Handshake-Mechanismus setzt weitergehende nationale Festlegungen über die dort beschriebene HTTP-Übermittlungsmethode voraus, um die störungsfreie Zusammenarbeit verschiedener Systeme sicherzustellen.

2.2.1 Übermittlungsmethode HTTP

Für die elektronische Übermittlung an die teilnehmenden Unternehmen nennen diese der Bundesnetzagentur die hierzu notwendigen Adressierungsinformationen (IP-Adresse), die diese an die bSn weiterreicht.

Die Port-Nummern des jeweiligen Empfängers (destination port) sind für HI-A und HI-B identisch und wie folgt zu verwenden. Sofern für die entsprechende Anfrage eine Anordnung notwendig ist, wird diese über denselbenPort übermittelt.

Anwendung	**destination port**
Beauskunftung von Verkehrsdaten	50200
Beauskunftung von Bestandsdaten	50210
Beauskunftung zur Standortfeststellung von mobilen Endgeräten	50220
Übermittlung der Anordnung zur Überwachung der Telekommunikation, Beauskunftung von Verkehrsdaten in Echtzeit	50230
~~Beauskunftung von Verkehrsdaten in Echtzeit~~	~~50240~~
Beauskunftung zur Struktur von Funkzellen	50250
Übermittlung von Rechnungsdaten bzw. Geltendmachung des Anspruchs auf Entschädigung nach § 23 Abs. 1 JVEG	50260

Sämtliche Nachrichten (Req, ReqAck, Res, ResAck, etc.) sind mittels POST-Methode in einer jeweils eigenen HTTP-Session zu übertragen. Die erfolgreiche Übertragung und serverseitige Validierung der XML-Nachricht wird vom Server durch ein HTTP 200 (OK) bestätigt. Nach Übertragung des HTTP-Statuscodes beendet der Server die Verbindung.

Eine Verbindung kann nach 60 Sekunden ohne Aktivität von Client oder Server beendet werden. Beendet der Server die Verbindung, übermittelt er zuvor HTTP 408 (Request Time-out) an den Client.

Je HTTP-Session ist nur eine Anfrage zulässig, mehrere Anfragen müssen in einzelnen HTTP-Sessions übermittelt werden.

Die Verwendung von „Content-Encoding: gzip“ innerhalb des HTTP-POST-Requests des Clients ist optional. Der Server muss entsprechende Requests und Responses verarbeiten können.

Sonderzeichen müssen gemäß XML-Standard durch die entsprechenden escape characters ersetzt werden, da sonst die Validierung fehlschlägt.

2.2.2 Behandlung von Fehlerfällen

2.2.2.1 Anfrage oder Auskunft ist fehlerhaft kodiert (nach ETSI TS 102 657, Abschnitt 5.1.5.3)

Wurde eine Anfrage/Auskunft formal fehlerhaft übermittelt (XML nicht valide oder Pflichtparameter sind nicht enthalten), ist die Annahme vom HTTP-Server mit dem **HTTP-Statuscode 422** (Unprocessable Entity) abzulehnen. Im HTTP-Body ist eine aussagekräftige Fehlermeldung zu übermitteln. Entspricht beispielsweise die Version der übermittelten Natparas nicht der erwarteten Version des Verpflichteten, ist im HTTP-Body der Fehlermeldung die beim Verpflichteten eingesetzte Version mitzuteilen.

Anlage A.4 in Teil A dieser TR TKÜV gilt bzgl. der Anforderungen an wiederholte Übermittlungsversuche einer Auskunft entsprechend.

2.2.2.2 Statusverletzungen (nach ETSI TS 102 657, Abschnitt 5.1.5.3)

Bei Statusverletzungen („falsche Meldungen zur falschen Zeit“) wird eine **Error Message** (ErrorAck) gesendet, die sich auf die *RequestID* des Requests bezieht und eine optionale Kommentierung ermöglicht.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData">
  <rdHeaderId> 0.4.0.2.3.0.14 </rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>123</authorisedOrganisationID>
      <requestNumber>10000</requestNumber>
    </requestID>
    <cSPID>001</cSPID>
    <timeStamp>20110830114353+0002</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <errorMessage>
      <information>status error: no request active for requestNumber
10000</information>
      <contactInformation/>
    </errorMessage>
  </retainedDataPayload>
</retainedDataMessage>
```

Beispiel einer Error-Message nach der ETSI-XSD

2.2.2.3 Anfrage kann nicht umgesetzt werden (nach ETSI TS 102 657, Abschnitt 5.1.5.2)

Kann eine Anfrage nicht umgesetzt werden (z.B. fehlerhafte Parameter, keine Übereinstimmung zur Anordnung oder bei einem *data-request* zu einem abgelehnten warrant), ist eine wie im nachfolgenden Beispiel aufgebaute *FailureResponse*-Nachricht mit einer Begründung zu versenden.

Demnach wird dieses Verfahren notwendig, wenn

a) bei der manuellen Überprüfung einer Request-Nachricht (z.B. nach Übermittlung einer Anordnung
oder der Abfrage von Bestandsdaten) festgestellt wird, dass die gesamte Anfrage nicht umgesetzt
werden kann oder

b) die automatische Prüfung (z.B. einer Request-Nachricht vom Typ *usageData*) einen Fehler der
Parameter feststellt.

Regelmäßig wird anschließend die Übermittlung einer neuen Anfrage unter einer neuen *requestNumber* nötig.

Diese FailureResponse-Nachricht kann ebenfalls genutzt werden, wenn technische oder andere Störungen beim verpflichteten Unternehmen die Beauskunftung verzögern und die anfragende Stelle darüber informiert werden soll.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage
xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData" >
  <rdHeaderId> 0.4.0.2.3.0.14 </rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>[…]</authorisedOrganisationID>
      <requestNumber>[RequestNumber des fehlerhaften requests]</requestNumber>
    </requestID>
    <cSPID>[…]</cSPID>
    <timeStamp>[…]</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <responseMessage>
      <responseStatus>
        <responseFailed>
          <information>[Fehlerbeschreibung]</information>
          <contactInformation>[optionale Kontaktdaten]</contactInformation>
```

```
        </responseFailed>
      </responseStatus>
    </responseMessage>
  </retainedDataPayload>
</retainedDataMessage>
                                        Die Felder […] sind entsprechend zu belegen.
```

Beispiel einer FailureResponse-Nachricht nach der ETSI-XSD

2.2.2.4 Versendung der ResponseComplete- bzw. –Incomplete-Nachricht

Treten keine Fehler auf, wird der Request vom Typ warrant mit der **ResponseComplete-Nachricht** bestätigt.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData">
  <rdHeaderId> 0.4.0.2.3.0.14 </rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>123</authorisedOrganisationID>
      <requestNumber>10000</requestNumber>
    </requestID>
    <cSPID>001</cSPID>
    <timeStamp>20110701165010+0001</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <responseMessage>
      <responseStatus>
        <responseComplete/>
      </responseStatus>
    </responseMessage>
  </retainedDataPayload>
</retainedDataMessage>
```

Beispiel einer Response-Nachricht nach der ETSI-XSD

Sind Teile der Anordnung nicht umsetzbar wird eine **ResponseIncomplete-Nachricht** versendet, die eine automatisch auswertbare Liste der als ungültig gewerteten einzelnen Kennungen enthält.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData">
  <rdHeaderId>0.4.0.2.3.0.14</rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>123</authorisedOrganisationID>
      <requestNumber>10000</requestNumber>
    </requestID>
    <cSPID>001</cSPID>
    <timeStamp>20100701165010+0001</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <responseMessage>
      <responseStatus>
        <responseIncomplete/>
      </responseStatus>
      <nationalResponsePayload>
        <countryCode>DE</countryCode>
        <headerID>0.4.0.2.3.0.9</headerID>
        <responseDetails>
          <rejectedTargets>
            <RejectedTargetNumber>7</RejectedTargetNumber>
            <RejectedTargetNumber>8</RejectedTargetNumber>
            <RejectedTargetNumber>16</RejectedTargetNumber>
          </rejectedTargets>
        </responseDetails>
      </nationalResponsePayload>
    </responseMessage>
```

```
  </retainedDataPayload>
</retainedDataMessage>
```

Beispiel einer ResponseIncomplete-Nachricht nach der ETSI-XSD (siehe auch Anlage A.2)

2.2.2.5 Wiederholte Zusendung der gleichen Message

Jede request-, response- oder cancel-Message wird durch eine entsprechende ACK-Message bestätigt. In Fällen, in denen diese ACK-Message ausbleibt, kann die gleiche ursprüngliche Message (z.B. ein request) inkl. der gleichen requestNumber erneut gesendet werden. Das jeweils empfangende System muss die Zusendung der gleichen Message erkennen können und

- eine ACK-Message zurücksenden,
- jedoch die weitere Bearbeitung der zweiten Message (z.B. die Beauskunftung von Verkehrsdaten) dann unterbinden, wenn die erste Message bereits empfangen wurde und sich in Bearbeitung befindet.

Die wiederholte Zusendung der Message muss inhaltsgleich erfolgen; würde ein optional durchgeführter Vergleich der vorliegenden und der wiederholten Message einen Unterschied ergeben, muss die weitere Verarbeitung abgebrochen und mit einem FailureResponse-Nachricht gemeldet werden.

2.2.2.6 Versendung einer cancel-Message

Mit einer cancel-Message können Behörden noch unbearbeitete Requests stoppen, um beispielsweise versehentlich verschickte oder in die Zukunft gerichtete dataRequests die nicht mehr benötigt werden, zu stoppen.

2.2.3 Festlegung zu den Formaten

Grundsätzlich sind die zu beauskunftenden Daten wenn möglich in dem Format zu beauskunften, in dem sie beim verpflichteten Unternehmen vorliegen. Soweit einzelne vorliegende Daten zur Beauskunftung erst in ein durch die ETSI-Spezifikation vorgegebenes Format umgewandelt werden müssen, ist die im nachfolgenden Abschnitt 2.2.3.3 gelistete Kodierung zu verwenden. Die berechtigten Stellen müssen die dort aufgeführten Kodierungen innerhalb ihrer Anfragen verwenden.

Da diese Festlegungen durch neu hinzukommende Nutzungen bzw. abfragbare Verkehrsdaten ergänzt werden müssen, gibt dieser Abschnitt den Stand bei der Herausgabe der entsprechenden Ausgabe der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Festlegungen mit den Betroffenen ab und ergänzt die Auflistung. Die jeweils aktuelle Version der Festlegungen zu den Formaten wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur unter (http://www.bundesnetzagentur.de/tku) zum Download bereitgestellt.

2.2.3.1 Formate für Datums- und Zeitangaben

Für diesen Teil der TR TKÜV ist die Nutzung der Kodierung *GeneralizedTime* für Datums- und Zeitangaben einheitlich vorgegeben. Dabei wird das Format von *GeneralizedTime* auf YYYYMMDDhhmmss.fraction +/- time-differential eingeschränkt, wobei YYYY dem Jahr entspricht, MM dem Monat, DD dem Tag, hh der Stunde (00 bis 23), mm der Minute (00 bis 59), ss der Sekunde (00 bis 59). Die Angabe einer höheren Genauigkeit (Sekundenbruchteile) ist optional. Die Zeitangabe muss grundsätzlich der amtlichen deutschen Zeit (=local time) entsprechen. Um unterschiedliche Zeiten beim Übergang zwischen Sommer- und Winterzeit unterscheidbar darstellen zu können, ist die Angabe der Zeitdifferenz zu UTC nötig. Diese Vorgabe gilt auch für die zu beauskunftenden Daten die in der eigenen Anlage bzw. im eigenen Netz des verpflichteten Unternehmens erzeugt werden; bei Zeitangaben von ausländischen Roamingpartnern kann abweichend die bereitgestellte Zeitangabe verwendet werden.

2.2.3.2 Formate für geografische Standortinformationen nach ETSI TS 102 657

Als Standardwert für die Koordinaten-Angaben sind geografische Koordinaten in dezimaler Schreibweise („*geoCoordinatesDec*“) oder geografische Winkelkoordinaten („*geoCoordinates*“) zu verwenden.

Die Koordinaten-Angabe erfolgt innerhalb der Struktur „*extendedLocation*“ auf Basis des Bezugssystems WGS84. Sofern bekannt, ist die Standortinformation unter Angabe der Hauptstrahlrichtung („*azimuth*“) zu erfolgen.

Sofern die Beschreibung eines geografischen Standortes, z.B. für eine sogenannte Funkzellenabfrage oder zur Erteilung der Auskunft zur Standortfeststellung von mobilen Endgeräten, mittels postalischer Angaben erfolgen muss, ist diese unter Verwendung des Parameters „*postalLocation*“ innerhalb der Struktur „*extendedLocation*“ mitzuteilen.

2.2.3.3 Formate der Funkzellenkennung für Funkzellenabfragen

Bei Funkzellenabfragen ist die angefragte Funkzellenkennung im Feld *„userLocationInformation“* zu übermitteln. Hierbei ist zu beachten, dass nur eine Angabe im *userLocationInformation-Block* enthalten sein darf. Die Verwendung anderer Datenfelder wie z.B. GlobalCellID ist nicht zulässig.

Für Funkzellenkennungen innerhalb von Verkehrsdatenauskünften ist ebenfalls ausschließlich das Feld *„userLocationInformation“* zu verwenden.

2.2.3.4 Formate für sonstige Kennungen nach ETSI TS 102 657

Die nachfolgende Tabelle A listet die Kennungen nach ETSI TS 102 657 zur Erläuterung deren Nutzung auf, für die lediglich eine Formatierungsmöglichkeit besteht.

Tabelle B enthält Kennungen, für die in der ETSI-Spezifikation grundsätzlich mehrere Formatierungs-möglichkeiten vorgesehen sind, oder bei denen eine Erläuterung hilfreich erscheint, und erläutert die Varianten, die nach der Vorgabe der obigen Erläuterung verwendet werden sollen bzw. für die requests der berechtigten Stellen verwendet werden müssen:

Tabelle A			
Kennung	**Format nach TS 102 657 (ggf. nationale Ergänzung)**	**Beispiel der Kodierung nach TS 102 657**	
PartyNumber (Rufnummer, MSISDN, VLR)	E.164 im internationalen Format als UTF-String	Kennung	0123/4567890
		ETSI-Format	491234567890
IMSI	Octet String Size 3-8 nach 3GPP TS 09.02	Kennung	262071234567890
		ETSI-Format	62021732547698F0

IMEI	Octet String Size 8 nach 3GPP TS 09.02[1]	Kennung	12345678901234
		ETSI-Format	21436587092143F0
~~Global Cell ID~~	~~Octet String Size 5-7 nach 3GPP TS 09.02~~	~~Kennung~~	~~262-07-01180-54689~~
		~~ETSI-Format~~	~~62F270049CD5A1~~
userLocationInformation	Octet String Size 1-35 nach 3GPP TS 29.274		
emailAddress (E-Mail Adresse)	UTF8String	Kennung	max.moritz@emailadresse.de
		ETSI-Format	max.moritz@emailadresse.de

[1] Liegen bei einer IMEI nur die Stellen 1 bis 14 vor, sind die restlichen Stellen mit dem Füllwert (11110000) bzw. „F0“ aufzufüllen. Beim Vergleich von IMEIs ist eine IMEI auch dann als äquivalent zu der angefragten IMEI zu betrachten, wenn die Prüf- oder Softwareversionsziffern abweichend oder nicht vorhanden sind.

Tabelle B			
Kennung	**Format nach TS 102 657**	**Beispiel der Kodierung nach TS 102 657**	
IPv4-Adresse	Octet String Size 4	Kennung	127.0.0.1
		ETSI-Format	7F000001
IPv6-Adresse	Octet String Size 16	Kennung	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
		ETSI-Format	20010DB885A308D313198A2E03707344

Für ansonsten benötigte Kennungen, für die die ETSI-Spezifikation keine entsprechenden Parameter bereithält, enthält das nationale XML-Modul *Natparas2* Erweiterungen für den ETSI-Parameter *nationalTelephonyPartyInformation* (siehe Abschnitt 3.2.2 dieser TR TKÜV). So sind die beiden ETSI-Parameter TelephonyDeviceID sowie subscriberID zugunsten der dort realisierten Möglichkeiten nicht zu verwenden.

2.2.3.5 Kombinierte Beauskunftung von Verkehrsdaten zum Telefon- und Internetzugangsdienst einer Kennung (optional)

Die ETSI-Spezifikation TS 102 657 unterscheidet grundsätzlich Beauskunftungen zu verschiedenen Diensten, wie zu Sprachdiensten und Internetzugangsdiensten. Zur Beauskunftung der Verkehrsdaten zum Telefondienst und zur Internetnutzung einer bestimmten Kennung (Fest- oder Mobilfunknummer) würde dadurch eine getrennte Beauskunftung notwendig werden.

Um eine doppelte Anfrage und Beauskunftung von Verkehrsdaten zu vermeiden, ist nach dieser TR TKÜV folgendes Verfahren optional möglich:

1. Im *warrant-request* sowie im *data-request* wird mit dem Parameter *usageData* mitgeteilt, ob die Verkehrsdaten für den Telefondienst oder den Internetzugangsdienst beauskunftet werden sollen. Werden hier beide möglichen *Werte = true* gesetzt, wird mit dem request eine kombinierte Beauskunftung angefordert.
2. Zur Übermittlung der Verkehrsdaten eines kombinierten requests wird das Feld *nationalTelephonyServiceUsage* der ETSI-Spezifikation so erweitert (siehe nachfolgende Markierung in fett), dass mit der Beauskunftung für den Telefondienst auch die Beauskunftung des Internetzugangsdienstes erfolgen kann.

```
TelephonyServiceUsage ::= SEQUENCE
{
 partyInformation    [1] SEQUENCE OF TelephonyPartyInformation OPTIONAL,
 communicationTime  [2] TimeSpan OPTIONAL,
  -- Time and duration of the communication
 nationalTelephonyServiceUsage[10] NationalTelephonyServiceUsage OPTIONAL
}
NationalTelephonyServiceUsage :: = SEQUENCE
{
    countryCode    [1] UTF8String (SIZE (2)),
    version        [2] UTF8String (SIZE (2)),
    internetAccess [3] NAServiceUsage OPTIONAL
}
```

Die Möglichkeit der Nutzung dieser Methode muss im Konzept angegeben werden. Unterstützt das verpflichtete Unternehmen diese Möglichkeit nicht, wird der entsprechende request mit einer Fehlermeldung nach Abschnitt 2.2.2.3 beantwortet.

2.2.4 Normierung der Antwortdaten bei Bestands- und Verkehrsdaten-Beauskunftungen

Eine nationale Abfrage bzgl. der Auswahl von geeigneten ETSI-Parametern für Bestands- und Verkehrsdaten ergab, dass die Spezifikation durchaus Interpretationsmöglichkeiten bietet und es deswegen in einigen Fällen zu abweichender Parameterauswahl kommen kann. Um eine bundesweit einheitliche Parameterauswahl realisieren zu können, legen die beiden nachfolgenden Tabellen für die bislang unterschiedlich angewandten Bestands- und Verkehrsdaten, die zu nutzenden Parameter herstellerübergreifend fest:

Tabelle A Bestandsdaten-Kriterium	**relativer Pfad zum auszuwählenden ETSI-Parameter**
Vertragsnummer	subscribedTelephonyServices/SubscribedTelephonyServices/serviceID
Zahlungsmethode (Postpaid, Prepaid)	PaymentDetails/billingMethod
Mandatsreferenz (SEPA-Lastschriftverfahren)	BankAccount/sepaRefNumber
Adressen	
Vertriebspartner	subscribedTelephonyServices/SubscribedTelephonyServices/ resellerAddress[1]
Service-Provider-Name[2]	subscribedTelephonyServices/SubscribedTelephonyServices/ otherAddresses/OtherAddress/addressComments
Anschlussinhaber	AddressInformation/relatedPersonName
Freitext für sonstige abweichende Adressangaben	AddressInformation/otherInformation
SIM-Karten- und Rufnummern	
SIM-Kartennummer(n)	SubscribedTelephonyServices/registeredICCIDs
Aktivierungsdauer einer Rufnummer	SubscribedTelephonyServices /registeredNumbersInfo/timeSpan
Deaktivierungsgrund	SubscribedTelephonyServices /registeredNumbersInfo/disableReason
Login-Informationen	
Benutzername	LoginInfo/login
Passwort	LoginInfo/password
Dienstetyp (z.B. E-Mail)	LoginInfo/serviceName
Gültigkeitsdauer des Benutzernamens / Passworts	LoginInfo/timeSpan
weitere Authentifikationsmethoden	LoginInfo/needsAdditionalAuthentication

[1]für die weiteren Angaben wie Straße, Hausnummer, PLZ und Ort sind die entsprechenden Parameter unterhalb dieses Pfades entsprechend zu verwenden.

[2] Sofern ein Service-Provider anzugeben ist, ist dies durch die Eintragung „Serviceprovider“ im Parameter otherAddresses/ OtherAddress/addressType zu signalisieren. Für die weieteren Angaben wie Straße, Hausnummer, PLZ und Ort sind die entsprechenden Parameter unterhalb des Pfades „OtherAddress/address/“ entsprechend zu verwenden.

Tabelle B Verkehrsdaten-Kriterium	**relativer Pfad zum auszuwählenden ETSI-Parameter**
Geo-Koordinaten	
Länge	/extendedLocation/spot/gsmLocation/geoCoordinates/longitude[1]
Breite	/extendedLocation/spot/gsmLocation/geoCoordinates/latitude[1]
Abstrahlrichtung	/extendedLocation/spot/gsmLocation/geoCoordinates/azimuth[1]
Datenvolumen	
Sendevolumen	nationalTelephonyServiceUsage/internetAccess/octetsUploaded
Empfangsvolumen[2]	nationalTelephonyServiceUsage/internetAccess/octetsDownloaded
Dienstetypen	
„CallType“,.„Call Indicator“ bzw. „Call Action Type“	TelephonyServiceUsage/operatorSpecificCallDetails
SMS	TelephonyPartyInformation/partyRole in Kombination mit. TelephonyServiceUsage/operatorSpecificCallDetails
MMS	TelephonyPartyInformation/partyRole in Kombination mit. TelephonyServiceUsage/operatorSpecificCallDetails
TEL / VIDEOTEL	TelephonyPartyInformation/partyRole in Kombination mit. TelephonyServiceUsage/operatorSpecificCallDetails
Datendienst	TelephonyPartyInformation/partyRole in Kombination mit. TelephonyServiceUsage/operatorSpecificCallDetails

[1] gilt für Koordinatenangaben im Bogenmaß (Grad, Minuten, Sekunden), für Koordinaten in dezimaler Notation sind die Parameter unterhalb der Struktur „geoCoordinatesDec“ entsprechend zu verwenden

[2] dieses Feld ist ebenfalls zu verwenden, falls keine richtungsgetrennten Daten vorliegen und nur das Gesamtvolumen berichtet werden kann. In diesem Fall ist das Feld octetsUploaded leer zu lassen.

2.2.5 Flexible Nutzung des Freitext-Feldes „otherInformation“

Für alle etwaigen Parameter, für die keine eindeutigen Entsprechungen in der ETSI-Struktur existieren, ist das Freitextfeld „otherInformation“ (responseMessage/responsePayload/ResponseRecord/additionalInformation/otherInformation) zu nutzen.

Die hierbei einzuhaltende Syntax ist dem Abschnitt 3.3.2.1 zu entnehmen.

3 Definition der nationalen Parameter

3.1 Allgemeines

Die dieser TR TKÜV zugrunde liegenden internationalen Standards und Spezifikationen verfügen über die Möglichkeit, nationale Parameter zu übermitteln.

Nachfolgend werden die zusätzlichen nationalen XML-Module '*Natparas2*' zur Übermittlung der Kopie der Anordnung sowie der ergänzenden Metadaten im *warrant*- und *data-request* sowie ‚*Natparas3*‘ zur Übermittlung der Antwort bei den sonstigen Nutzungen (z.B. für die Standortfeststellung von Mobilfunkendgeräten) festgelegt. Änderungen bzw. Erweiterungen sind nur durch die Bundesnetzagentur möglich.

Sonderzeichen müssen gemäß XML-Standard durch die entsprechenden escape-characters ersetzt werden, da sonst die Validierung fehlschlägt.

Das Modul *Natparas2* wird im Feld *NationalRequestParameters* der *RequestMessage* eingefügt, das Modul *Natparas3* wird im Feld *NationalResponsePayload* der *ResponseMessage* eingefügt.

Die jeweils aktuellen Versionen der nationalen Module werden auf der Webseite der Bundesnetzagentur (http://www.bundesnetzagentur.de/tku) veröffentlicht und gelten ab dem Tag der Veröffentlichung. Die veröffentlichten Natparas-Versionen sind hierbei nicht an die

jeweils aktuelle ETSI-XSD-Version gekoppelt. Sofern jedoch Versionen der nationalen Module beispielsweise aufgrund von XML-Kompatibilitätsproblemen mit bestimmten ETSI-XSD-Versionen nicht zu verwenden sind, erfolgt auf der Webseite ein entsprechender Hinweis.

Verpflichtete, deren TK-Dienste von Änderungen der nationalen Module nicht betroffen sind, müssen neuere Versionen nicht zwingend in ihren Anlagen einpflegen. Daher müssen berechtigte Stellen grundsätzlich alle Versionen vorhalten, um auch alle Anwendungsfälle in der Praxis abdecken zu können. Zur Verwendung verschiedener Versionen wird mit dieser Ausgabe der TR TKÜV eine einheitliche Versionierung für die Module eingeführt.

3.2 Beschreibung des nationalen XML-Moduls 'Natparas2' (für Anfragen)

Diese Anlage enthält die XML-Beschreibung des nationalen Moduls *'Natparas2'* zur Übermittlung der Kopie der Anordnung (AO) sowie der ergänzenden Metadaten im *warrant-* und *data-request*.

Da diese XML-Beschreibung durch neu hinzukommende Parameter ergänzt werden muss, gibt die Anlage nur den Stand bei der Herausgabe der entsprechenden Ausgabe der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Parameter mit den Betroffenen ab und ergänzt das XML-Modul. Die jeweils aktuelle Version der XML-Beschreibung der nationalen Parameter sowie der nachfolgenden Festlegung der einzelnen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur unter (http://www.bundesnetzagentur.de/tku) zum Download bereitgestellt.

3.2.1 Festlegung der Nutzungsarten

Das Modul Natparas2 ist für folgende Nutzungsarten festgelegt:

- Übermittlung der Anordnung sowie der Metadaten (Typ *warrant*);
  hierbei dient die ETSI-*RequestMessage* lediglich als Übermittlungshülle
- Übermittlung der konkreten Abfragen zur Beauskunftung von Bestands- und Verkehrsdaten (Typen *subscriberData* und *usageData*);
  hierbei enthält das nationale Modul lediglich ergänzende Daten während in der ETSI-*RequestMessage* die eigentliche Abfrage durch die Belegung der entsprechenden bekannten Parameter (z.B. Übermittlung der Rufnummer und eines Zeitraums bei der Beauskunftung von Verkehrsdaten) enthalten ist
- Übermittlung von Anfragen zur Standortfeststellung von mobilen Endgeräten (Typ *locating*) und zur Struktur von Funkzellen (Typ *radioStructure*);
  hierbei dient die ETSI- *RequestMessage* lediglich als Übermittlungshülle
- Übermittlung der Aktivierungs- oder Änderungsnachrichten zur Umsetzung von TKÜ-Maßnahmen (Typ *lawfulInterception*);
  hierbei dient die ETSI- *RequestMessage* lediglich als Übermittlungshülle

Die an eine Anordnung gekoppelten Nutzungsarten können im *warrant-request* mehrere Kennungen enthalten (Kennzeichnung der verschiedenen Kennungen durch den Parameter <*targetNumber*> als laufende Nummer). Für die Nutzungsarten *usageData*, *locating* und *radioStructure* ist pro Request nur eine Kennung erlaubt.

3.2.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas2

Das XML-Modul *Natparas2* wird im Feld *NationalRequestParameters* der *RequestMessage* eingefügt und ist wie folgt strukturiert:

3.2.2.1 Festlegungen zum Header

NationalRequestParameters Parameter	Beschreibung	M/ C/O
<countryCode>	Belegung „DE“	M
<headerID>	Versionsnummer des nationalen Moduls Natparas2 Das Format der Versionsnummer setzt sich wie folgt zusammen aus: ETSI-Version.TR-Ausgabe.Nr, wobei: ETSI-Version: 8 Zeichen, TR-Ausgabe: 4 Zeichen, Nr: 2 Zeichen. Beispiel: 01.17.01.07.0.01 bedeutet: **01.17.01** | **07.0** | **01** ETSI TS 102 657 Versionsnr 01.17.01 | relevante TR TKÜV-Ausgabe 7.0 | fortlaufende Nummerierung für die NatParas-Version	M
<referencedRequestNumber>	Entspricht der RequestNumber (RequestID in der ETSI-XSD) einer zuvor übermittelten Anordnung im warrant-request; Pflichtparameter für alle auf einen warrant-requests folgenden requests.	C
<targetNumber>	Laufende Nummer der betroffenen Kennung im warrant-request, auf die in den *subscriberData*- und *lawfulInterception*-Requests verwiesen wird, um die Beauskunftung bzw. TKÜ-Maßnahme zu einer Kennung einzuleiten. Der Parameter ist in diesen Fällen ein Pflichtparameter.	C
<groupID>	Die laufende Nummer ~~dient~~ ist ausschließlich zur ~~der~~ Gruppierung verschiedener Anfragen für Rechnungszwecke zu verwenden. (z.B. zur Gruppierung von 10 Beauskunftungen zu je einer IP-Adresse nach § 23 Abs. 1 Anlage 3 Nr. 201 JVEG)	O
<additionalInformation>	Freitext, der vor der Bearbeitung der Anwendungen <subscriberData>, <locating> und <radioStructure> berücksichtigt werden muss.	O
<requestDetails>	An dieser Stelle werden die möglichen Anwendungsmodule als *choice* eingefügt	M

requestDetails Parameter	Beschreibung	M/ C/O
<warrant>	zur Übermittlung einer Anordnung inkl. der Metadaten	C
<usageData>	für Anfragen nach Verkehrsdaten, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden; die nationale Ergänzung nach Abschnitt 3.2.2.3 enthält zusätzlich die Unterscheidung nach dem abgefragten Dienst (Telefon- oder Internetzugangsdienst)	C
<subscriberData>	für Anfragen nach Bestandsdaten, die über die Abfragemöglichkeiten der ETSI-XSD hinaus gehen	C
<locating>	für Standortortbestimmungen von Mobilfunkendgeräten	C
<radioStructure>	für Anfragen zur Struktur von Funkzellen, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden	
<lawfulInterception>	für die Aktivierung/Modifizierung/Deaktivierung einer TKÜ-	C

	Maßnahme nachdem die Anordnung übermittelt wurde	
<compensation>	Datentyp zur Geltendmachung von Entschädigungsansprüchen	C

3.2.2.2 Festlegungen zum warrant-request für die nationale XSD-Ergänzung

Warrant Parameter	Beschreibung	M/ C/O
<warrantTIFF>	Anordnung (base64-codierte TIFF-Dokument wie oben beschrieben)	C
<warrantDate>	Datum der Anordnung im Format YYYYMMDD	M
<warrantTargets>	Liste der einzelnen Kennungen mit laufender Nummerierung, → siehe Definition <WarrantTarget>	M
<legalBases>	Rechtliche Grundlage der Anordnung → siehe XSD-Definition	M
<warrantTextform>	Umsetzung der geforderten Textform bei Bestandsdatenanfragen gem. § 113 Abs. 2 TKG, als Alternative zum TIFF-Dokument	C

WarrantTarget Parameter	Beschreibung	M/ C/O
<targetNumber>	Laufende Nummer zur Identifikation der Kennung innerhalb der Metadaten und darauf bezogene requests	M
<target>	Hier wird das Element *TelephonyPartyInformation* mit den entsprechenden Datenbelegungen aus der ETSI-XSD sowie bei Bedarf der Parameter *nationalTelephonyPartyInformation* mit den nationalen Ergänzungen aus dem XSD-Modul Natparas2 eingefügt	M
<startDateTime>	Beginn des in der Anordnung für diese Kennung genannten Zeitraums, Format *GeneralizedTime*	M
<endDateTime>	Ende des in der Anordnung für diese Kennung genannten Zeitraums, Format *GeneralizedTime*	M
<targetType>	Die Angabe dient zur Unterscheidung, ob • für die Kennung eine Verkehrsdatenbeauskunftung oder eine TKÜ-Maßnahme angefordert wird, • sich die Verkehrsdatenbeauskunftung in Kombination mit dem Parameter <usageData> auf *<telephonyService>, auf <dataService> oder auf eine kombinierte Anfrage bezieht,* • *sich die TKÜ-Maßnahme* in Kombination mit dem Parameter <interceptionCriteria> *auf Voice+Data oder IRIOnly bezieht.*	M
<interceptionCriteria>	Pflichtfeld bei TKÜ-Maßnahmen; gibt den möglichen Umfang der Überwachung gemäß der Anordnung an (CC+IRI oder IRIOnly). Der in diesem Rahmen tatsächlich zu aktiverende Umfang wird mit dem activation-request eingestellt (dadurch wird es beispielsweise möglich, eine für CC+IRI bestehende Anordnung, aus von der berechtigten Stelle zu vertretenden Gründen, lediglich als IRIOnly-Maßnahme umzusetzen).	C

WarrantTextform Parameter	Beschreibung	M/ C/O
<originator>	Name des Anfragestellers.	M
<originatorContactDetails>	Telefonnummer des Anfragestellers.	M
<endOfText>	Notwendiges Textfeld, um den Abschluss der Textform erkenntlich zu machen. Als Parameter-Wert ist „Dieses Dokument ist ohne Unterschrift gültig!“ einzutragen.	M

NationalTelephonyPartyInformation Parameter	Beschreibung	M/ C/O

<countryCode>	Belegung „DE“	M
<headerID>	Versionsnummer des nationalen Moduls Natparas2 Das Format der Versionsnummer setzt sich wie folgt zusammen aus: ETSI-Version.TR-Ausgabe.Nr, wobei ETSI-Version: 8 Zeichen, TR-Ausgabe: 4 Zeichen, Nr: 2 Zeichen. Beispiel: 01.17.01.07.0.01 bedeutet: **01.17.01** ETSI TS 102 657 Versionsnr 01.17.01 / **07.0** relevante TR TKÜV-Ausgabe 7.0 / **01** fortlaufende Nummerierung für die NatParas-Version	M
<partyNumberAKUE>	Die in der Anordnung anzugebende ausländische Rufnummer, beginnend mit der Landeskennzahl (z.B. 33 für Frankreich)	C
<voipID>	VoIP-Kennung, die nicht dem E.164-Format entspricht (z.B. max.moritz@voiptelefon.de	C
<lineID>	Leitungskennung bzw. Technical Key eines Internetzugangsweges	C
<userName>	Accountname eines Internetzugangs	C
<postBoxAddress>	Postfachadresse bzw. Accountname eines E-Mail Postfachs	C
<macAddress>	Macadresse eines Endgerätes zum Internetzugang bei Kabelnetzen	C
<ipAddress>	Feste IP-Adresse eines Internetzugangs	C

3.2.2.3 Festlegungen zum usageData-request für die nationale XSD-Ergänzung

Für die Beauskunftung von Verkehrsdaten werden innerhalb der ETSI-XSD die Anfragedaten zu den konkret zu beauskunftenden Verkehrsdaten übermittelt (z.B. Übermittlung der Rufnummer und eines Zeitraums bei der Beauskunftung von Verkehrsdaten).

Die nationale XSD-Ergänzung enthält neben den grundsätzlichen Angaben im Header (u.a. mit dem Verweis auf den *warrant-request* und die betreffende *targetNumber*) die Angabe zum abgefragten Dienst (Telefondienst, Datendienst, kombinierte Anfrage).

UsageData Parameter	Beschreibung	M/ C/O
~~<usageData>~~	~~Kennzeichnung, ob zu einer Fest- oder Mobilfunknummer Verkehrsdaten aus dem Telefondienst oder dem Internetzugangsdienst beauskunftet werden sollen. Werden beide Möglichkeiten gesetzt, liegt eine kombinierte Beauskunftung nach Kapitel 2.2.3.4 vor.~~ ~~Mögliche Werte:~~ ~~- *telephonyService*: true oder false~~ ~~- *dataService*: true oder false~~	~~M~~
<usageData>	Kennzeichnung, ob zu einer Fest- oder Mobilfunknummer Verkehrsdaten aus dem Telefondienst oder dem Internetzugangsdienst beauskunftet werden sollen. Werden beide Möglichkeiten gesetzt, liegt eine kombinierte Beauskunftung nach Kapitel 2.2.3.5 vor. Mögliche Werte: - *telephonyService*: true oder false - *dataService*: true oder false - *lateRecordRequest*: true oder false - zielwahl*Request*: true oder false Besonderer *data-request* zur Beauskunftung von verspäteten Verkehrsdaten (Late-record), die erst nach einer Wartezeit und nach dem Ablauf des abgefragten Zeitraums im warrant-	M

	request zur Verfügung stehen. *zielwahlRequest* zur Kennzeichung einer Zielwahlsuche.	

3.2.2.4 Festlegungen zum subscriberData-request für die nationale XSD-Ergänzung

Für die Beauskunftung von Bestandsdaten werden innerhalb der ETSI-XSD die Anfragemerkmale zu den konkret zu beauskunftenden Bestandsdaten übermittelt (z.B. Übermittlung der Rufnummer oder eines Namens mit Adresse).

3.2.2.5 Festlegungen zum locating-request für die nationale XSD-Ergänzung

Für die Beauskunftung von Anfragen zur Standortfeststellung in Mobilfunknetzen dient die ETSI-XSD lediglich als Übermittlungshülle sowie zur Festlegung einer *requestNumber*; die nationale XSD-Ergänzung enthält das Suchriterium. Für den loacting-request gilt das Verfahren nach Abschnit 1.3.1. Durch den Eintrag der <referencedRequestNumber> im Header des location-requests wird der Bezug zum w*arrant-request* hergestellt.

Falls zusätzlich zu dem Ortungsergebnis auch eine Beauskunftung über die Struktur der ermittelten Funkzelle erfolgen soll, so ist diese eigenständig mittels eines *radioStructure-requests* durchzuführen.

Locating Parameter	Beschreibung	M/ C/O
<mSISDN>[1]	Rufnummer des zu lokalisierenden Mobilfunkendgerätes im Format E.164; siehe Festlegungen im Abschnitt 2.2.3.~~3~~4	C
<iMSI>[1]	IMSI des zu lokalisierenden Mobilfunkendgerätes im Format 3GPP TS 09.02; siehe Festlegungen im Abschnitt 2.2.3.~~3~~4	C
<vLR>[1]	VLR-Kennnung im Format E.164; ; siehe Festlegungen im Abschnitt 2.2.3.~~3~~4. Die Angabe erfolgt nur in Kombination mit einer iMSI-Kennung	C
<legalBases>	Rechtliche Grundlage der Beauskunftung → siehe XSD-Definition	C

[1] Bei nationalen Mobilfunkanschlüssen muss das Feld <mSISDN>, bei ausländischen Mobilfunkanschlüssen das
Feld <iMSI> und - *sofern vom Netzbetreiber gefordert* - zusätzlich das Feld <vLR> gefüllt werden.

3.2.2.6 Festlegungen zum radioStructure-request für die nationale XSD-Ergänzung

Für die Beauskunftung zur Struktur von Funkzellen wird ~~einer~~ der ~~nachfolgend gelisteten~~ Parameter
userLocationInformation der ETSI-XSD genutzt~~:~~

Hierbei ist zu beachten, dass bei Funkzellenanfragen nur eine Angabe im userLocationInformation-Block enthalten sein darf.

- ~~globalCellID,~~
- ~~eCGI,~~
- ~~extendedLocation.~~

3.2.2.7 Festlegungen zum lawfulInterception-request für die nationale XSD-Ergänzung

Durch die verschiedenen Varianten des lawfulInterception-requests werden die mittels eines *warrant-requests* übermittelten und vom Unternehmen freigegebenen TKÜ-Administrierungen aktiviert, modifiziert, deaktiviert oder verlängert bzw. nach einer Unterbrechung erneuert.

Hierfür wird eines der nachfolgend beschriebenen Module aus der ETSI-XSD eingefügt.

LawfulInterception Parameter	Beschreibung	M/ C/O
<activation>	Zur Aktivierung einer freigegebenen TKÜ-Maßnahme (warrant-request) → siehe Definition <Activation>	C

<renewal> [1]	Zur Verlängerung einer TKÜ-Maßnahme; setzt die Freigabe eines weiteren warrant-requests voraus. → siehe Definition <Renewal>	C
<modification>	Zur Modifizierung einer TKÜ-Maßnahme, wenn hierzu keine Anordnung notwendig wird (z.B. Änderung der Ausleiteadresse) → siehe Definition <Modification>	C
<deactivation>	Zur vorfristigen Deaktivierung einer TKÜ-Maßnahme → siehe Definition <Deactivation>	C

[1] ~~Die Anwendung <renewal> wird auch zur gerichtlichen Bestätigung einer staatsanwaltschaftlichen Eilanordnung genutzt. Dabei wird zunächst diese Eilanordnung mit einem warrant-request und anschließenden <activation> aktiviert und nach Zusendung der gerichtlichen Anordnung mittels weiterem warrant-request durch den anschließenden <renewal> bestätigt bzw. verlängert.~~ *Die Anwendung von <renewal> wird auch zur gerichtlichen Bestätigung einer staatsanwaltschaftlichen Eilanordnung genutzt. Dabei wird zunächst diese Eilanordnung mit einem warrant-request unter Verwendung des Parameters needsConfirmation und anschließende~~*nm* *<activation> aktiviert und nach Zusendung der gerichtlichen Anordnung mittels weiterem warrant-request durch den ~~anschließenden~~ darauf folgenden <renewal> bestätigt bzw. verlängert.*

Activation Parameter	Beschreibung	M/ C/O
<target>	zu überwachende Kennung → Für diesen Parameter wird der Parameter telephonyPartyInformation aus der ETSI-XSD verwendet	M
<lIID>	Enthält die zu verwendende LIID. Verpflichteten Unternehmen, denen aufgrund des Betriebs älterer Vermittlungs, die Vorgabe der LIID durch die Bundesnetzagentur ausdrücklich zugestanden wurde, melden in der Response-Nachricht die tatsächlich aktivierte LIID.	C
<interceptionCriteria>	Details zum Umfang der Überwachung, → siehe Definition <InterceptionCriteria>	M
<monitoringCenter>	Details zu den Ausleitungszielen, → siehe Definition <MonitoringCenter>	M
<startDateTime> [2]	Zeitpunkt der geplanten Aktivierung der Maßnahme, Format GeneralizedTime. Nichtangabe bedeutet unverzügliche Aktivierung	C
<endDateTime> [2]	Zeitpunkt der geplanten Abschaltung, Format GeneralizedTime	M

[2] Diese Werte können von den durch den warrant-request vorgegebenen Werten abweichen, müssen sich jedoch in dem durch diese ursprünglichen Werte definierten Zeitrahmen befinden.

Renewal Parameter	Beschreibung	M/ C/O
<lIID>	LIID der Maßnahme	M
<endDateTime>	Zeitpunkt des neuen Endzeitpunkts, Format *GeneralizedTime*	M

Modification Parameter	Beschreibung	M/ C/O
<lIID>	LIID der Maßnahme	M
<newLIID>	Neue LIID, sofern diese geändert werden soll	C
<newInterceptionCriteria>	Neue Daten für das Feld InterceptionCriteria, sofern der Umfang der TKÜ-Maßnahme geändert werden soll	C
<newMonitoringCenter>	Neue Daten für das Feld MonitoringCenter, sofern die Ausleitungsziele geändert werden sollen	C

Deactivation Parameter	Beschreibung	M/ C/O
<lIID>	LIID der Maßnahme	M
<endDateTime>	Zeitpunkt der geplanten Abschaltung, Format *GeneralizedTime*. Nichtangabe des Parameters bedeutet unverzügliche Abschaltung	C

InterceptionCriteria Parameter	Beschreibung	M/ C/O
<interceptVoice> [1]	gibt an, ob der Telefondienst überwacht werden soll	M
<interceptData> [1]	gibt an, ob der Internetzugangsdienst überwacht werden sollen	M
<interceptIdlemodeHandover>	gibt an, ob Handover eines Mobilfunkendgeräts auch im Idlemode überwacht werden sollen	C

[1] Sind beide Werte ‚false', wird eine IRIOnly-Maßnahme angefordert.

MonitoringCenter Parameter	Beschreibung	M/ C/O
<destinationNumber>	HI3-Ausleitungsziel für Sprache, Format E.164	C
<ipAddress>	HI3-Ausleitungsziel für Daten, der Port ergibt sich aus Teil A	C

	der TR TKÜV	
~~<portNumber>~~	~~Portnumber 50000 oder 50010 entsprechend den Vorgaben im Teil A, Anlagen C und D dieser TR TKÜV~~	~~C~~
<ftpAddress>	IP-Adresse des HI2-Ausleitungsziels	C
<ftpUsername>	FTP-Benutzername für das HI2-Ausleitungsziel	C
<ftpPassword>	FTP-Passwort für das HI2-Ausleitungsziel	C
<x25address>	X25-Adresse des HI2-Ausleitungsziels	C
<x31address>	X31-Adresse des HI2-Ausleitungsziels	C

3.3 Beschreibung des nationalen XML- Moduls 'Natparas3' (für Antworten)

Diese Anlage enthält die XML-Beschreibung des nationalen Moduls *'Natparas3'* zur Übermittlung zusätzlicher Antwortdaten (z.B. für die Standortfeststellung von Mobilfunkendgeräten) in der Response-Message.

Da diese XML-Beschreibung durch neu hinzukommende Parameter ergänzt werden muss, gibt die Anlage nur den Stand bei der Herausgabe der entsprechenden Version der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Parameter mit den Betroffenen ab und ergänzt das XML-Modul. Die jeweils aktuelle Version der XML-Beschreibung der nationalen Parameter sowie der nachfolgenden Festlegung der einzelnen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur unter (http://www.bundesnetzagentur.de/tku) zum Download bereitgestellt.

3.3.1 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3

Das Modul *Natparas3* ist für folgende Nutzungsarten festgelegt:

- Übermittlung der Antwortdaten zur Standortfeststellung von mobilen Endgeräten (Typ */locatingResult*) und zur Struktur von Funkzellen (Typ *radioStructureResult*); hierbei dient die ETSI-ResponseMessage lediglich als Übermittlungshülle.
- Übermittlung ergänzender Antwortdaten zur Beauskunftung nach Bestandsdaten; je nach Umfang der Abfrage dient die ETSI- ResponseMessage lediglich als Übermittlungshülle oder enthält ergänzende Informationen.
- Übermittlung der Bestätigung von Aktivierungs- oder Änderungsvorgängen zur Umsetzung von TKÜ-Maßnahmen (Typ *lawfulInterceptionResult*); hierbei dient die ETSI- ResponseMessage lediglich als Übermittlungshülle. Diese Übermittlung dient der Rückantwort auf administrativer Ebene und ersetzt die nach Teil A, Anlage A.3 der TR TKÜV vorgesehenen HI1-Nachrichten, die vom verpflichteten Unternehmen dann optional deaktiviert werden kann.

3.3.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3

Das XML-Modul Natparas3 wird im Feld *NationalResponsePayload* der *ResponseMessage* eingefügt und ist wie folgt strukturiert:

3.3.2.1 Festlegungen zum Header

<table>
<tr><th colspan="3">NationalResponsePayload
Parameter</th><th>Beschreibung</th><th>M/
C/O</th></tr>
<tr><td colspan="3"><countryCode></td><td>Belegung „DE“</td><td>M</td></tr>
<tr><td colspan="3"><headerID></td><td>Versionsnummer des nationalen Moduls Natparas3

Das Format der Versionsnummer setzt sich wie folgt zusammen aus:

ETSI-Version.TR-Ausgabe.Nr,

wobei
ETSI-Version: 8 Zeichen,
TR-Ausgabe: 4 Zeichen,
Nr: 2 Zeichen.

Beispiel: 01.17.01.07.0.01 bedeutet:

<table><tr><td>01.17.01</td><td>07.0</td><td>01</td></tr></table></td><td>M</td></tr>
</table>

	ETSI TS 102 657 Versionsnr 01.17.01	relevante TR TKÜV-Ausgabe 7.0	fortlaufende Nummerierung für die NatParas-Version	
<additionalInformation>	Freitext für besondere Angaben des verpflichteten Unternehmens zur Beauskunftung			O
<additionalDocument>	Möglichkeit als Ergänzung ein zusätzliches Dokument zu übermitteln			O
<responseDetails>	An dieser Stelle werden die möglichen Anwendungsmodule eingefügt.			M

Das Feld *additionalInformation* kann (analog zu Abschnitt 2.2.5) wie nachfolgend beschrieben mit verschiedenen Informationen befüllt werden:

<Info> →<List>

<Info> →<Comment>

<Info> →<List>;<Comment>

<List> →**<ListItem>**

<List> →**<ListItem>;<List>**

<ListItem> →**„<Feldname>“=„<FeldWert>“**

<Comment> →**COMMENT=<text>**

Die o.g. Bezeichner in spitzen Klammern sind dabei als Nichtterminale zu lesen. Für die Parameter <Feldname>, <FeldWert> und <text> sind beliebige Strings zulässig.

Sofern bei den Parametern <Feldname> und <FeldWert> doppelte Anführungszeichen oder Backslash-Zeichen vorkommen, sind diese Zeichen jeweils per Backslash zu escapen.

Der Parameter <Comment> ermöglicht zusätzlich zu den netzbetreiberspezifischen Feldern Freitextkommentare.

Ein Beispiel ohne Freitext wäre:

”Gesuchtes Kriterium“=”12345“;”Zeitraum“=”01.05.2015 00:00:00 – 02.05.2015 23:59.59-”;”Carrier Id”=”66221”

Das gleiche Beispiel mit Freitext:

”Gesuchtes Kriterium“=”12345“;”Zeitraum“=”01.05.2015 00:00:00 – 02.05.2015 23:59.59-”;”Carrier Id”=”66221”;COMMENT=Die Zellinformationen wurden bereits teilweise gelöscht, weil die Daten älter als 7 Tage sind.

Für fehlende Parameter ist das Freitextfeld „otherInformation“ der ETSI-XSD nach Abschnitt 2.2.5 zu verwenden.

responseDetails Parameter	Beschreibung	M/ C/O
<locatingResult>	für Ergebnisse bei Standortortbestimmungen von Mobilfunkendgeräten; sind der Kennung mehrere SIM-Karten zugeordnet, muss dieser Parameter je SIM-Karte belegt und als jeweils eigenständiges <locatingResult> in den <responseDetails> übermittelt werden	C
<radioStructureResult>	für Rückmeldungen auf Anfragen zur Struktur von Funkzellen, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden	C
<lawfulInterceptionResult>	für Rückmeldungen auf die Aktivierung/Modifizierung/Deaktivierung einer TKÜ-Maßnahme, nachdem die Anordnung übermittelt wurde	C
<rejectedTargets>	Hier sind abgelehnte Targets anzugeben. Sofern mehrere targets abgelehnt wurden, ist das Element <RejectedTargetNumber> entsprechend zu verwenden	C

3.3.2.2 Festlegungen zu locatingResult für die nationale XSD-Ergänzung

Für die Anwendung vom Typ *locating* wird eine locatingResult je SIM-Karte aufgeführt. Sind der im locating-request angegebenen Kennung mehrere SIM-Karten zugeordnet, wird der Parameter locatingResult mit den jeweiligen Antwortparametern pro SIM-Karte in den Header eingebunden.

locatingResult Parameter	Beschreibung	M/ C/O
<mSISDN>	Rufnummer des georteten Mobilfunkendgeräts im Format E.164, Format nach Abschnitt 2.2.3.~~3~~4	C
<iMSI>	IMSI der georteten SIM-Karte im Format 3GPP TS 09.02, Format nach Abschnitt 2.2.3.~~3~~4	C
<iMEI>	IMEI des georteten Mobilfunkendgeräts im Format 3GPP TS 09.02, Format nach Abschnitt 2.2.3.~~3~~4	C
<loginStatus>	Angabe des Zustandes des mobilen Endgerätes (attached bzw. registered oder detached bzw. unregistered)	C
<detachReason>	Grund der Ausbuchung als Freitext, z.B. „Ausschalten durch Teilnehmer“	C
<vLR>	VLR-Kennung im Format E.164, Format nach Abschnitt 2.2.3.~~3~~4	C
<lastRadioContact>	Zeitpunkt des letzten Funkkontakts im Format GeneralizedTime, Format nach Abschnitt 2.2.3.1	C
<transmitterDetails>	Angabe der Netztechnologie (GSM oder UMTS) → siehe Definition der ETSI-XSD (Parameter *TransmitterDetails*)	C
<userLocationInformation>	im Format nach 3GPP TS 09.02, Format nach Abschnitt 2.2.3.~~3~~4	C
<extendedLocation>	Zur Übermittlung der geografischen Koordinaten des Standorts der Antenne → siehe Definition in der ETSI-XSD (Parameter *ExtendedLocation*) nach der Maßgabe des Abschnittes 2.2.3.2	C
<postalLocation>	Postalische Angabe des Standorts der Antenne bei zusätzlicher Mitteilung der postalischen Adresse zu den geografischen Koordinaten → siehe Definition in der ETSI-XSD (Parameter *postalLocation*)	C

Die Kennzeichnung als „conditional“ bezieht sich auf die Reichweite der Rechtsgrundlage der Abfrage.

3.3.2.3 Festlegungen zu radioStructureResult für die nationale XSD-Ergänzung

radioStructureResult Parameter	Beschreibung	M/ C/O
<radiationPattern>	grafische Darstellung des theoretischen Versorgungsbereiches (base64-codiertes TIFF-Dokument)	M

3.3.2.4 Festlegungen zu lawfulInterceptionResult für die nationale XSD-Ergänzung

lawfulInterceptionResult Parameter	Beschreibung	M/ C/O
<lIID>	Referenznummer	M
<begin>	Aktivierungszeitpunkt der Überwachung Datum und Uhrzeit im Format *GeneralizedTime* nach Abschnitt 2.2.3.1	C
<end>	Deaktivierungszeitpunkt der Überwachung Datum und Uhrzeit im Format *GeneralizedTime* nach Abschnitt 2.2.3.1	C
<modification>	Modifizierungszeitpunkt der Überwachung Datum und Uhrzeit im Format *GeneralizedTime* nach Abschnitt 2.2.3.1	C

3.3.2.5 Festlegungen zu subscriberDataResult für die nationale XSD-Ergänzung

Die Beauskunftung von Bestandsdaten bezieht sich auf den speziellen *subscriberDataRequest* nach Abschnitt 3.2.2.4 und erfolgt grundsätzlich innerhalb der ETSI-XSD. Um die Referenz zum Request herzustellen, wird zudem die Übermitlung des Headers nach Abschnitt 3.3.2.1 notwendig.

Zur eigentlichen Beauskunftung eines *subscriberData-Requests* wird für den Telefondienst der Parameter *TelephonySubscriber* der ETSI-XSD verwendet, der die Möglichkeit enthält, mehrere Vertragsdaten (z.B. Verträge für unterschiedliche Mobilfunknummern) in einer Response zu übermitteln. So erfolgt auch die Beauskunftung der Merkmale *billingMethod*, *bankAccount, billingAddress* oder *contractPeriod* innerhalb der ETSI-XSD.

Um ergänzende Daten pro Vertrag bzw. Mobilfunknummer zu übermitteln, ist das Feld *NationalResponsePayload* nicht geeignet, da es pro Response nur einmal verwendet werden kann. Für vertragsspezifische Ergänzungen ist daher der Paramter nationalTelephonySubscriptionInfo im Parameter *TelephonySubscriber* der ETSI-XSD wie folgt zu ergänzen:

<table>
<tr><th colspan="3">nationalTelephonySubscriptionInfo</th></tr>
<tr><th>Parameter</th><th>Beschreibung</th><th>M/
C/O</th></tr>
<tr><td><countryCode></td><td>Belegung „DE“</td><td>M</td></tr>
<tr><td><headerID></td><td>Versionsnummer des nationalen Moduls Natparas-3

Das Format der Versionsnummer setzt sich wie folgt zusammen aus:

ETSI-Version.TR-Ausgabe.Nr

wobei
ETSI-Version: 8 Zeichen,
TR-Ausgabe: 4 Zeichen
Nr: 2 Zeichen

Beispiel: 01.17.01.07.0.01 bedeutet:

<table><tr><th>01.17.01</th><th>07.0</th><th>01</th></tr><tr><td>ETSI TS 102 657 Versionsnr 01.17.01</td><td>relevante TR TKÜV-Ausgabe 7.0</td><td>fortlaufende Nummerierung für die NatParas-Version</td></tr></table></td><td>M</td></tr>
<tr><td><pIN></td><td>PIN der abgefragten Kennung</td><td>C</td></tr>
<tr><td><other></td><td>Freitext zur Beauskunftung weiterer Abfragen entsprechend dem Parameter <other> im subscriberDataRequest</td><td>C</td></tr>
</table>

Der nachfolgende Auszug der ETSI-XSD zeigt die Struktur des Parameters *TelephonySubscriber* mit verschiedenen Möglichkeiten der Beauskunftung von Bestandsdaten.

```
TelephonySubscriber ::= SEQUENCE
{
    subscriberID                  [1] TelephonySubscriberId OPTIONAL,
        -- unique identifier for this subscriber, e.g. account number
    genericSubscriberInfo         [2] GenericSubscriberInfo OPTIONAL,
        -- generic personal information about this subscriber
[...]
    subscribedTelephonyServices       [4] SEQUENCE OF SubscribedTelephonyServices
OPTIONAL,
        -- a subscriber (or account) may have more than one service listed against them
    ...,
    nationalTelephonySubscriberInfo  [5] NationalTelephonySubscriberInfo OPTIONAL
        -- To be defined on a national basis
        -- Only to be used in case the present document cannot fulfil the national
requirements
}
```

```
SubscribedTelephonyServices ::= SEQUENCE
{
[...]
    timeSpan                          [3] TimeSpan OPTIONAL,
        -- Start and end data, if applicable, of the subscription
    registeredNumbers                 [4] SEQUENCE OF PartyNumber OPTIONAL,
        -- The set of telephone numbers registered for this service
[...]
    iMSI                               [9] IMSI OPTIONAL,
    pUKCode                           [13] UTF8String OPTIONAL,
    pUK2Code                          [14] UTF8String OPTIONAL,
    iMEI                              [15] SEQUENCE OF IMEI OPTIONAL,
    nationalTelephonySubscriptionInfo  [16] NationalTelephonySubscriptionInfo OPTIONAL,
        -- To be defined on a national basis
        -- Only to be used in case the present document cannot fulfil the national
requirements
    paymentDetails                    [17] PaymentDetails OPTIONAL
}
```

Auszug aus der ETSI-XSD TS 102 657

3.3.2.6 Kennzeichnung der Datensätze nach Datenherkunft

Im Parameter *NationalRecordPayload* muss für jeden Datensatz eine Auswahl getroffen werden, ob die Daten nach § 96 oder §113b TKG beauskunftet werden. Gleichermaßen wird hierdurch die Verpflichtung nach § 113c Abs. 3 Satz 2 TKG erfüllt.

NationalRecordPayload Parameter	Beschreibung	M/ C/O
<tKG113b>	Die beauskunfteten Datensätze waren nach §113b TKG gespeichert	M
<tKG96>	Die beauskunfteten Datensätze waren nach §96 TKG gespeichert	M

4 Übermittlung von Rechnungsdaten bzw. Geltendmachung des Anspruchs auf Entschädigung nach § 23 Absatz 1 JVEG

4.1 Grundsätzliches

Dieser Abschnitt beschreibt die technischen Einzelheiten zur optionalen gesicherten elektronischen Übermittlung von Rechnungsdaten bzw. der Geltendmachung von Ansprüchen auf Entschädigung im Vorfeld der eigentlichen Entschädigung nach § 23 Absatz 1 JVEG.

4.2 Methoden der elektronischen Übermittlung

Die Methode basiert auf der Nutzung der ETSI-Spezifikation TS 102 657 sowie der in diesem Teil der TR TKÜV festgelegten Bestimmungen.

Die Übermittlung ermöglicht es den verpflichteten Unternehmen, die in einem bestimmten Zeitrahmen angefallenen Rechnungsdaten nach § 23 Absatz 1 JVEG zum Abgleich an die betreffenden berechtigten Stellen zu versenden. Die Rechnungsdaten enthalten die verarbeiteten RequestNummern (beispielsweise einer Verkehrsdatenbeauskunftung oder einer Aktivierung einer Kennung) sowie die aus Sicht des verpflichteten Unternehmens vorgesehenen Kosten- und Rabbatierungsansätze.

Die standardisierte Übermittlung dieser Rechnungsdaten ermöglicht den berechtigten Stellen einen automatischen Abgleich mit den selbst vorliegenden Daten. Die weiteren Schritte (Bestätigung, Besprechung von Abweichungen etc.) sind aufgrund der hohen diesbezüglichen Diversität nicht Bestandteil dieser Schnittstelle.

Die Übermittlung der Rechnungsdaten erfolgt mit dem nationalen XML-Modul *Natparas2,* welches hierzu im Feld *NationalRequestParameters* der *RequestMessage* eingefügt wird.

4.3 Beschreibung des nationalen XML- Moduls 'Natparas2' (für Rechnungsdaten)

Dieser Abschnitt enthält die Beschreibung der XML-Elemente zur Übermittlung der Rechnungsdaten der verpflichteten Unternehmen an die berechtigten Stellen in einer Request-Message. Hierbei dient die ETSI-RequestMessage lediglich als Übermittlungshülle. Eine Response-Nachricht ist für diesen Anwendungsfall nicht vorgesehen.

Für die Übermittlung per HTTP sowie die Behandlung von Fehlerfällen gelten die Vorgaben des Abschnittes 2.2 entsprechend.

Da diese XML-Beschreibung durch neu hinzukommende Parameter ergänzt werden muss, gibt die Anlage nur den Stand bei der Herausgabe der entsprechenden Version der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Parameter mit den Betroffenen ab und ergänzt das XML-Modul entsprechend. Die jeweils aktuelle Version der XML-Beschreibung der nationalen Parameter sowie der nachfolgenden Festlegung der einzelnen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur unter (http://www.bundesnetzagentur.de/tku) zum Download bereitgestellt.

Festlegung der ergänzenden Daten

Compensation Parameter	Beschreibung	M/ C/O
<compensationName>	Freitext zur eindeutigen Beschreibung der Rechnungsdaten (z.B. für einen bestimmten Monat mit laufender Nummer für eine etwaige korrigierte nochmalige Zusendung)	M
<compensationItem>	→ siehe 4.3.1.1	M

Festlegungen zum Parameter *CompensationItem*

CompensationItem Parameter	Beschreibung	M/ C/O
<requestNumber>	Die RequestID, für die eine Entschädigung geltend gemacht werden soll (z.B. für eine Beauskunftung von Verkehrsdaten oder für die Aktivierung einer Überwachungsmaßnahme)	M
<groupID>	Hiermit werden nur die RequestIDs gekennzeichnet, die nach Maßgabe der Regelungen des § 23 Abs. 1 JVEG im Block verrechnet werden [1]	M
<jVEG2017~~3~~>	Auswahlfeld im nationalem Modul zur Nummer des Kostenansatzes, z.B. 'JVEG Nummer 102'	M
<rebate>	Kennzeichnung, ob für den Kostenansatz ein 20%-Rabatt aufgrund der zentralen Kontaktstelle berücksichtigt wurde Mögliche Werte: - *Rabatt berücksichtigt: true* - *Rabatt nicht berücksichtigt: false*	
<quantity>	Menge bzw. Multiplikator des Kostenansatzes [2]	M
<price>	Letztendlicher Kostenansatz für die jeweilige aufgeführte RequestID unter Berücksichtigung von Rabattierung und Multiplikator	M
<comment>	Freitext für zusätzliche Kommentare	O

[1] Werden beispielsweise in demselben Verfahren acht IP-Adressen abgefragt (Nr. 201 nach Anlage 3 zu § 23 Abs. 1 JVEG), so müssen die acht RequestIDs der einzelnen Abfragen gelistet werden, wobei die gleiche groupID zu verwenden ist. Der Kostenansatz nach § 23 JVEG Absatz 1 ist nur bei nur bei einer RequestID aufzuführen; bei den anderen RequestID ist der Betrag „0“ einzutragen.

[2] Dieser beträgt im Regelfall „1“. In mengenmäßigen Abrechnungen (z.B. für die Entschädigung von Leitungskosten nach Nummer 104) wird der notwendige Multiplikator als Intergerwert eingetragen.

Anlage A.1 ~~Anlage zu~~Erläuterungen ~~des~~ zum Verfahren~~s~~

Anlage A.1 enthält weiterführende Erläuterungen und Veranschaulichungen zum Verfahren.

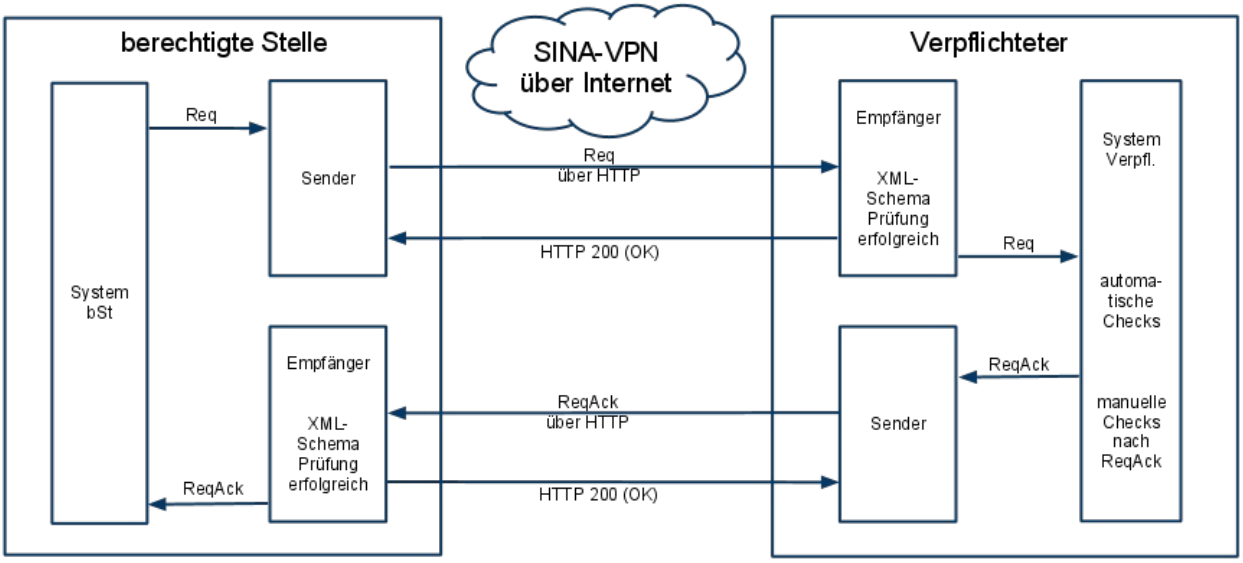
Beispielhafte Datensätze für die verschiedenen Anwendungsfälle sowie die jeweils aktuellen Versionen der nationalen XML-Module *Natparas2* und *Natparas3* sind auf unserer Webseite unter http://www.bundesnetzagentur.de/tku abrufbar.

Anlage A.1.1 Prinzipieller Kommunikationsfluss

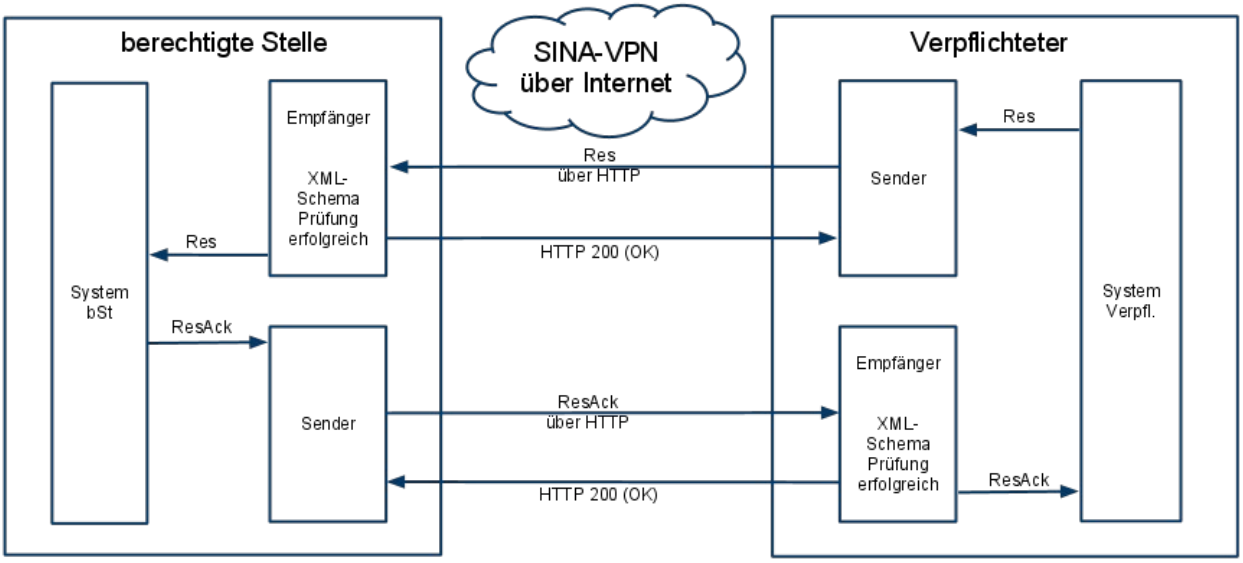
Die nachfolgenden Darstellungen sollen die grundsätzlichen Nutzungen der Schnittstelle in Ergänzung zu den Darstellungen in der ETSI TS 102 657 erläutern.

Aufteilung in System, Sender und Empfänger:

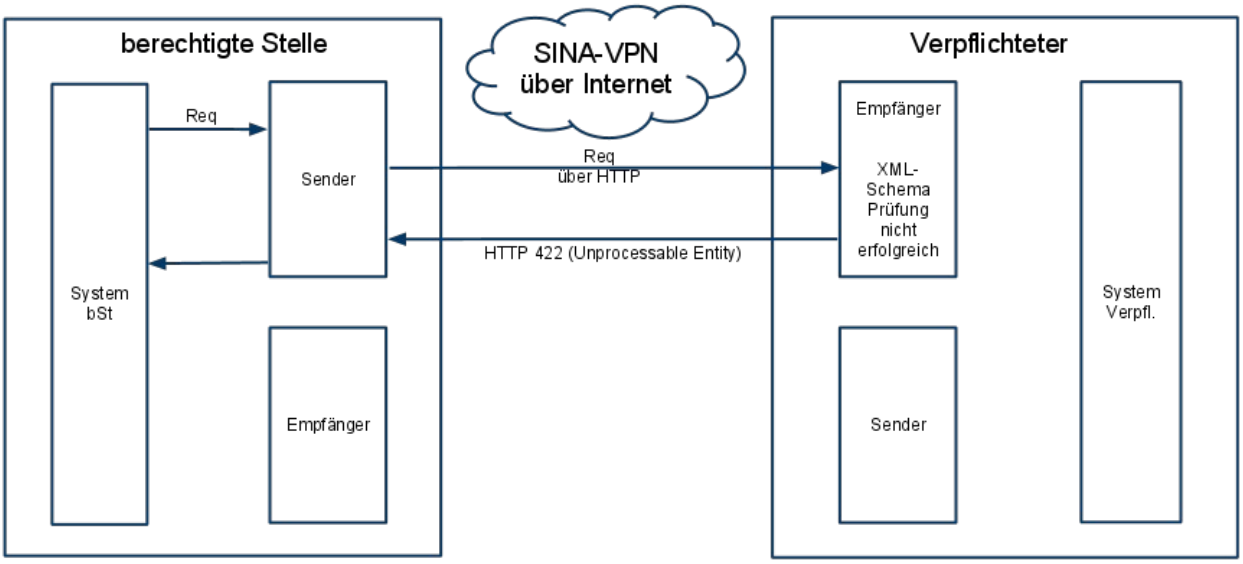
a) erfolgreiche Übermittlung eines Requests



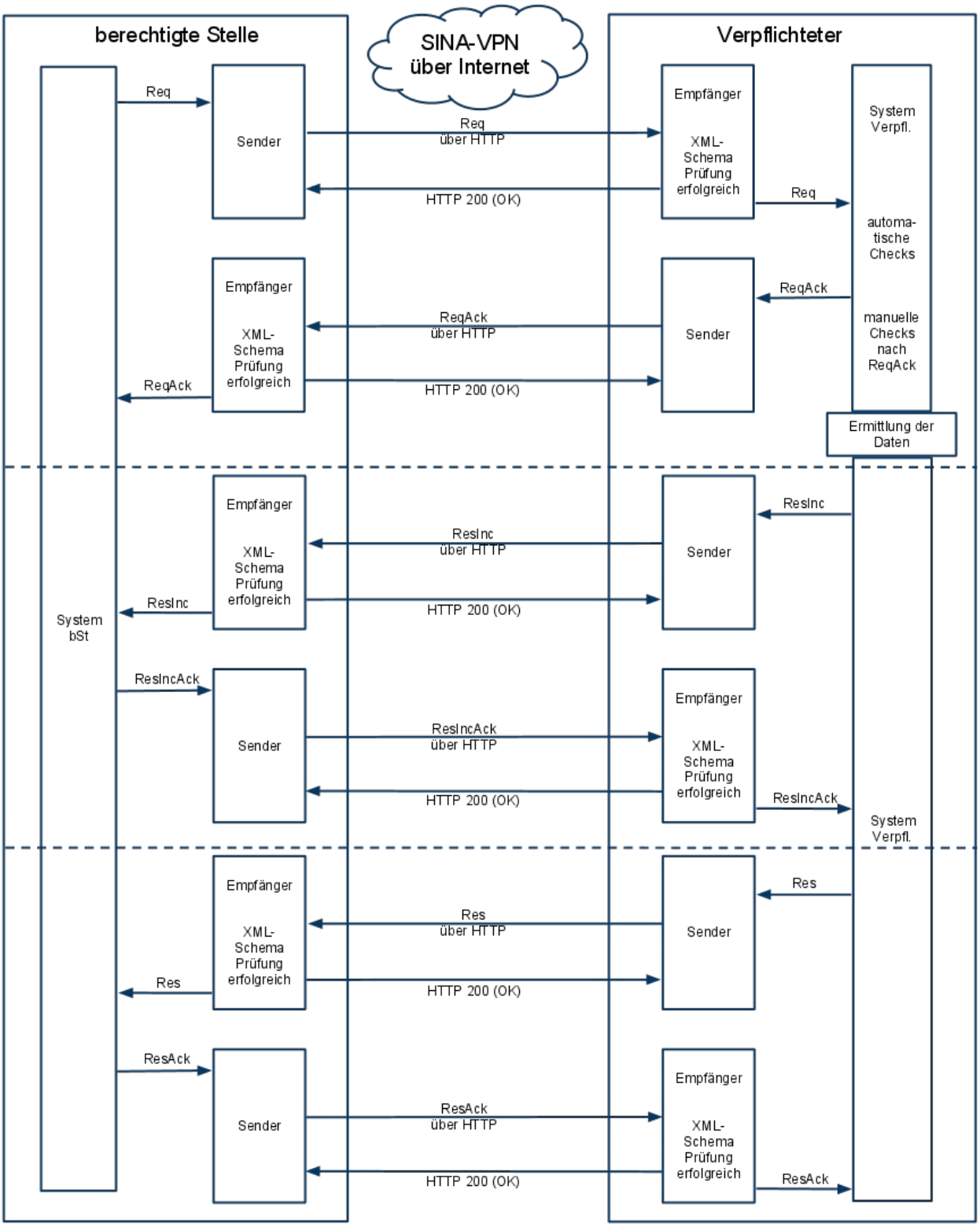
b) erfolgreiche Übermittlung einer Response



c) Übermittlung einer fehlerhaften Nachricht (Fehlerfall 5.1.5.3)
Die Darstellung zeigt beispielhaft eine fehlerhafte Request-Nachricht. Dieser Fall kann bei allen Arten von Nachrichten (Req, ReqAck, etc.) auftreten.



d) erfolgreiche Übermittlung eines Requests und multi-part Responses nach Abschnitt 5.2.3 der ETSI TS 102 657



Anlage A.1.2 Festlegungen zur Teilnahme am IP-VPN mittels Einsatz eines Kryptosystems

Allgemeines

Zum Schutz des IP-basierten Übergabepunktes werden dedizierte Kryptosysteme auf der Basis der IPSec-Protokollfamilie eingesetzt, um die Teilnetze der bSn und der Verpflichteten zu einem Virtual Private Network (VPN) zu verbinden. Zur Verwaltung der zur Authentisierung dienenden kryptographischen Schlüssel wird eine Public Key Infrastructure (PKI) eingerichtet, die von der Bundesnetzagentur als zentrale Zertifizierungs- und Registrierungsstelle betrieben wird. Darüber hinaus verwaltet die Bundesnetzagentur die möglichen Sicherheitsbeziehungen innerhalb einer Access Control List (ACL), die mittels eines Verzeichnisdienstes bereitgestellt wird.

Die Kryptosysteme werden als dedizierte Systeme jeweils vor den zu schützenden Teilnetzen der bSn und der Verpflichteten platziert. Die Systeme garantieren Authentisierung, Integrität und Verschlüsselung.

Darüber hinausgehende Mechanismen zum Schutz des Übergabepunktes, wie z.B. gegen Denial of Service-Attacken bei den bSn, werden durch die Kryptosysteme nur bedingt erfüllt und müssen durch die Betreiber der jeweiligen Teilnetze eigenständig gelöst werden.

Die jeweiligen Kryptosysteme sind grundsätzlich Bestandteile der technischen Einrichtungen der bS bzw. des Verpflichteten; insofern fällt der Betrieb (z.B. Betrieb eines SYSLOG-Servers) sowie die Wartung und Entstörung in die Zuständigkeit des jeweiligen Betreibers des Teilnetzes.

Die Anforderungen an die Kryptosysteme müssen ggf. künftig dem jeweiligen Stand der Technik angepasst werden, um das Schutzniveau weiterhin zu garantieren. Diesbezügliche Erweiterungen (z.B. Nutzung anderer Schlüssellängen) bzw. kurzfristig notwendige Änderungen der bestehenden Implementierung bei nachträglich entstandenen Sicherheitsmängeln sind von den Betreibern der jeweiligen Kryptosysteme in einem im Einzelfall festzulegenden Zeitraum - im Rahmen der von den Herstellern der Kryptosysteme zur Verfügung gestellten Erweiterungen bzw. Updates - nach Vorgabe durch die Bundesnetzagentur durchzuführen.

Netzarchitektur

Die Kryptosysteme der bSn und der Verpflichteten bilden ein Maschennetz, wobei stets gerichtete Sicherheitsbeziehungen (Punkt-zu-Punkt-Verbindungen) zwischen den TKA-Vn der Verpflichteten und den Teilnetzen der bSn etabliert werden. Verbindungen zwischen den Verpflichteten untereinander sind nicht möglich.

Die notwendigen Zertifikatsschlüssel zur Authentisierung der Kryptosysteme werden durch die Bundesnetzagentur erzeugt und nach erfolgter Registrierung auf der von den Betreibern der jeweiligen Teilnetze bereitgestellten SmartCard des Kryptosystems gespeichert. Die Schlüssel zur Verschlüsselung der zu übertragenden Daten werden eigenständig durch die Kryptosysteme pro etabliertem VPN erzeugt.

Nach der Inbetriebnahme der Kryptosysteme bauen diese eigenständig eine gesicherte Verbindung zum Verzeichnisdienst der Bundesnetzagentur auf, um die aktuelle ACL zu laden. Die weiteren Aktualisierungsprozesse der ACL erfolgen automatisch oder gesteuert durch die Bundesnetzagentur.

Die durch die Kryptosysteme erzeugten Logdaten (z.B. Erfolg eines ACL-Updates, Störung) werden im Standardformat SYSLOG (UDP-Port 514) zur Weiterbearbeitung an den Log-Server des Verpflichteten bzw. der bS geleitet.

Gestaltung des Internetzugangs bzw. Übergabepunktes

Um die Eindeutigkeit der Adressierung der VPN-Endpunkte sowie der sendenden und empfangenden Einrichtungen der Verbindungsstrecke zur Übermittlung der Überwachungskopie bzw. der IRI sowie der Daten gemäß Teil B herzustellen, werden öffentliche IP-Adressen eingesetzt. Werden vorhandene Intranetstrukturen verwendet, muss i.d.R. ein separates Tunneling eingesetzt werden, um die Schutzanforderungen zu erfüllen. Prinzipiell sind jedoch verschiedene Netzkonfigurationen möglich.

Die genannten Anforderungen sind bei der Beschreibung der Gestaltung des Internetzugangs bzw. Übergabepunktes im Rahmen des einzureichenden Konzeptes zu berücksichtigen.

Einsatzszenarien und Verfahrensablauf

Im Regelverfahren sind die Kryptosysteme fester Bestandteil der Teilnetze und u.a. über ihre IP- Konfiguration eindeutig innerhalb der ACL definiert. Nach erfolgter Registrierung und Schlüsselerzeugung wird der Verzeichnisdienst aktualisiert.

Eine Liste der für die Verwaltung der ACL notwendigen Daten sowie eine Beschreibung des Gesamtprozesses (Policy) wird für die am Verfahren Beteiligten bereitgestellt.

Im Konzept sind alle Details (z.B. die für die Übermittlung vorgesehene IP-Adresse) zu nennen, damit die ACL entsprechend gepflegt werden kann.

Sonstige Regelungen und Hinweise zur Teilnahme am IP-VPN

Neben diesen Regelungen zur Teilnahme am IP-VPN gelten die nachfolgenden normativen Einzelregelungen bzw. Hinweise:

- Regelungen für die Registrierung- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
  Die Anlage X.3 gibt den Stand bei Herausgabe dieser Ausgabe der TR TKÜV wieder.
- Hinweispapier 'Einbindung der IP-Kryptosysteme in die Netzinfrastruktur der Verpflichteten und der berechtigten Stellen'
- Antrag zur Teilnahme am IP-VPN für die Verpflichteten sowie für die bSn (Registrierung und technische Beschreibung der Infrastruktur des Teilnetzes mit IP-Adressen und Optionsauswahl)

Die Dokumente stehen auf der Homepage der Bundesnetzagentur im Sachgebiet Telekommunikation unter dem Stichwort Technische Regulierung Telekommunikation / Technische Umsetzung von Überwachungsmaßnahmen zum Download bereit.

Tabelle der einsetzbaren IP-Kryptosysteme

Diejenigen Systeme, die die systemtechnischen Basisanforderungen sowie die Anforderungen zur Interoperabilität erfüllen, werden in der folgenden Tabelle gelistet.

Die aktuelle Tabelle wird auf der Downloadseite der Bundesnetzagentur (http://www.bundesnetzagentur.de/tku) bereitgestellt.

Nr.	Hersteller	Produktname	Ansprechpartner
1	**secunet Security Networks AG** Ammonstraße 74 01067 Dresden www.secunet.com	SINA Box	Division Public Authorities E-Mail: Info@secunet.com Tel: 0201/5454-0

Anlage B Übermittlungsverfahren E-Mail-ESB

Diese Anlage beschreibt die nationalen Anforderungen an das Übermittlungsverfahren E-Mail-ESB.

1.1 Grundsätzliche Verfahrensbeschreibung

Der Einsatz des Übermittlungsverfahrens E-Mail-ESB richtet sich nach den Abschnitten 1 bis 3 dieses Teils der TR TKÜV.

Vor einer Nutzung des Übermittlungsverfahrens ~~der~~ E-Mail-ESB ~~muss~~müssen nach Benachrichtigung der bS über das Vorliegen einer Anordnung oder eines sonstigen Ersuchens zunächst die ersuchende bS und der Verpflichtete ihre ~~der~~ öffentlichen Schlüssel ~~der ersuchenden bS und der Verpflichteten~~ ausgetauscht ~~werden~~, die im Verschlüsselungsverfahren verwendet werden sollen. Eine zentrale Vorhaltung der Schlüssel z.B. über einen ~~(~~Key-Server~~)~~ ist für dieses Verfahren nicht vorgesehen. Der Verpflichtete muss sich vergewissern, dass der ih~~r~~m übermittelte Schlüssel von der anfragenden bS stammt, z.B. mittels einer telefonischen Überprüfung des Fingerprints.

Neben der Anordnung oder des sonstigen Ersuchens können die bSn Erläuterungen zu den abgefragten Verkehrsdaten (z.B. Zielwahlsuche, Echtzeitausleitung) und den Abfragezeiträumen (Zeitpunkte der Beauskunftungen, Nachlieferung von late records nach Ablauf des angeordneten Zeitraums) zur Erleichterung der Bearbeitung übermitteln. Die Bearbeitung richtet sich grundsätzlich nach den diesbezüglichen Ausführungen zum Übermittlungsverfahren ETSI-ESB.

Bei Einsatz des Übermittlungsverfahrens E-Mail-ESB sind ausschließlich solche Softwarelösungen zu verwenden, welche ein Verschlüsselungsverfahren nach dem gemäß RFC4880 spezifizierten OpenPGP-Verfahren in hybrider Anwendung ermöglichen. Der OpenPGP-Standard unterstützt die gängigsten Kryptoverfahren und –algorithmen~~,~~ ~~beispielsweise RSA und AES~~. Für die Nutzung ist eine asymmetrische RSA-Verschlüsselung mit einer Schlüssellänge von mindestens 4096 Bit ~~(asymmetrische Verschlüsselung)~~ mit einer symmetrischen AES-Verschlüsselung von mindestens ~~bzw.~~ 256 Bit ~~(symmetrische Verschlüsselung)~~ zu verwenden. Die Aufzeichnungsanschlüsse der bSn müssen diese Verfahren unterstützen. Der Betrieb der E-Mail-ESB außerhalb der bSn, der Verpflichteten oder deren Erfüllungsgehilfen sind nicht zulässig.

Andere Verschlüsselungsverfahren, die proprietäre PGP- oder andere Ende-zu-Ende-Verschlüsselungen verwenden, sind nicht zulässig. Müssen seitens der bS geheimhaltungsbedürftige Unterlagen übermittelt werden (z.B. eine als Verschlußsache eingestufte richterliche Anordnung) obliegt es der bS, über eine dezidierte Verschlüsselung dieser Unterlage zu entscheiden (z.B. mit der Verschlüsselungssoftware Chiasmus) und diese in Absprache mit dem betroffenem Unternehmen mittels der E-Mail-ESB zu übersenden. Das Verschlüsselungsverfahren nach dem OpenPGP-Standard bleibt davon unberührt.

Ist das Übermittlungsverfahren E-Mail-ESB nicht im Abfragesystem integriert, muss die Verbindung zwischen Abfragesystem und E-Mail-ESB über eine Transportsicherung nach Abschnitt 4.1 des Anforderungskatalogs nach § 113f TKG verfügen. Ein Datentransport zwischen den Einrichtungen per Datenträger (z.B. USB-Stick) ist nicht zulässig. Zudem muss die Anforderung- der automatischen Protokollierung nach § 35 TKÜV auch hierbei sichergestellt sein. ~~Eine Übermittlung per USB ist nicht zulässig.~~

Zum Schutz vor dem Zugriff aus dem Internet:

- darf ~~das Übermittlungsverfahren E-Mail-ESB sowie~~ die für das Übermittlungsverfahren E-Mail-ESB ~~hierfür~~ eingesetzte Hardware- und softwarekomponente für keinen anderen Zwecke eingesetzt werden,
- ist das Übermittlungsverfahren E-Mail-ESB nach der Verwendung vom Internet zu entkoppeln und
- muss zwischen dem Übermittlungsverfahren E-Mail-ESB und dem Internetanschluss eine Firewall eingesetzt werden.

Zudem sind die im Übermittlungsverfahrens E-Mail-ESB anfallenden Klardaten nach der Übermittlung aus dem RAM ~~irreversibel~~ zu löschen. Außerdem muss eine Auslagerung auf

eine Festplatte oder beispielsweise in einen Ordner für „Gesendete Objekte“ o.ä. verhindert werden (Abschnitt 3.2.~~1.~~2 im Teil B).

Nach § 113c Abs. 3 Satz 2 TKG sind Verkehrsdaten, die nach § 113b TKG gespeichert waren bei der Übermittlung an die bS zu kennzeichnen. Hierzu ist jeder einzelne Verkehrsdatensatz mit dem Syntax „tKG§ 113b ~~TKG~~“ zu kennzeichnen. Zu übermittelnde betrieblich gespeicherte Verkehrsdaten sind mit dem Syntax „tKG§ 96 ~~TKG~~“ zu kennzeichnen.

Die bSn können mit Übermittlung der Anordnung oder in einer separaten E-Mail die Beauskunftung von verspäteten Verkehrsdaten (Late-records) festlegen, die erst nach einer Wartezeit und nach dem Ablauf des abgefragten Zeitraums der Anordnung zur Verfügung stehen. Die mit der Bundesnetzagentur abzustimmende Wartezeit muss so bemessen sein, dass Late-records regelmäßig vollständig erfasst werden. Die Beauskunftung dieser Late-records erfolgt nach dieser Wartezeit und enthält ggf. auch alle zu diesem Zeitpunkt für den gesamten Zeitraum gespeicherten Verkehrsdaten. Diese Festlegung kann durch die bSn mittels einer erneuten E-Mail zurückgezogen werden.

Teil X

Informativer Anhang

Der Teil X enthält die geplanten Änderungen in der TR TKÜV, die Grundlage der Diskussion der nächsten Ausgabe werden sollen sowie ergänzende Informationen zu den verschiedenen Anlagen dieser Ausgabe.

Anlage X.1 Geplante Änderungen der TR TKÜV

Dieser Anhang ist nicht verbindlich im Sinne des § 110 Abs. 3 TKG. Es wird lediglich über zukünftig geplante Änderungen informiert, deren Notwenigkeit erst nach Abschluss der Erarbeitung dieser Ausgabe bekannt geworden ist. Diese geplanten Änderungen sollen bei der Erarbeitung der nächsten Ausgabe der TR TKÜV abgestimmt werden.

Bei der Erbringung des Nachweises nach § 110 Abs. 1 Nr. 3 TKG wird die Bundesnetzagentur Implementierungen auf Basis dieses informativen Anhanges als technisch korrekt anerkennen.

Die geplanten Änderungen sind in die Kopie des jeweiligen Textauszugs eingetragen und durch fette Kursivschrift und Unterstreichung markiert.

Anlage X.2 Vergabe eines Identifikationsmerkmals für bS zur Gewährleistung von eindeutigen Referenznummern

Grundsätzliches

Gemäß § 7 Abs. 2 Satz 1 TKÜV hat jedes verpflichtete Unternehmen jede bereitgestellte Überwachungskopie durch die von der bS vorgegebene Referenznummer der jeweiligen Überwachungsmaßnahme zu bezeichnen, sofern der bS diese Kopie über Telekommunikationsnetze mit Vermittlungsfunktionen übermittelt wird.

Die Referenznummer setzt sich gemäß der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜV) und den zugrunde liegenden ETSI- und 3GPP-Spezifikationen aus maximal 25 Stellen zusammen.

Als nutzbarer Zeichenvorrat sind grundsätzlich alle Groß- und Kleinbuchstaben, alle Ziffern sowie die Zeichen '-', '_' und '.', vorgesehen. Bei Verwendung von ISDN-Stichen zur Übermittlung der Kopie der Nutzinformation sind jedoch lediglich die Ziffern '0' bis '9' erlaubt.

Bedingt durch die Implementierung der ETSI-Schnittstelle und die damit verbundene Änderung der Administrierungsoberfläche ist die Vorgabe der Referenznummer durch die bSn mittlerweile weitgehend möglich.

Mögliche Problemfälle

Verschiedene Netzelemente sind jedoch darauf angewiesen, dass keine Maßnahmen mit identischer Referenznummer administriert werden. In der Praxis kann es bedingt durch gleiche Referenznummern unterschiedlicher berechtigter Stellen in diesen Fällen zu Uneindeutigkeiten und somit zu möglichen technischen Fehlfunktionen der Überwachungstechnik bei der Zuordnung und Übermittlung von Überwachungskopien kommen. So können beispielsweise Ausleitungen von Kopien der Nutzinformationen zu den bSn ganz oder teilweise ausfallen.

Gewährleistung von eindeutigen Refernznummern

Um die Eindeutigkeit sicherzustellen und somit einen fehlerfreien Betrieb der Übermittlungsanlagen zu gewährleisten, ist ein zusätzliches Identifikationsmerkmal innerhalb der Referenznummer notwendig. Dieses Identifikationsmerkmal stellt die Unterscheidung der bSn sicher, die ihrerseits die Stellen der verbleibenden Referenznummer selbstständig als eineindeutiges Merkmal der Überwachungsmaßnahme vergeben.

Daher teilt die Bundesnetzagentur jeder berechtigten Stelle einmalig eine dreistellige bS-ID zu.

Bei künftigen TKÜ-Maßnahmen wird diese bS-ID an den ersten drei Stellen der Referenznummer verwendet, sofern das zur Umsetzung der Anordnung verpflichtete Unternehmen bereits die ETSI-Implementierung eingeführt hat. Die bS teilt dem Verpflichteten jeweils die gesamte Referenznummer inklusive der bS-ID mit.

Demnach setzt sich die gesamte Referenznummer wie folgt zusammen:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

bS-ID	**22 Stellen zur Vergabe einer eindeutigen Referenznummer je bS** *Erlaubte Zeichen, grundsätzlich: "**a**"..."**z**", "**A**"..."**Z**", "**-**", "**_**", "**.**", und "**0**"..."**9**"* *Erlaubte Zeichen bei ISDN-Ausleitung: "**0**"..."**9**" bei*

Die zugeteilte bS-ID wird ebenfalls für die Schnittstelle zur technischen Umsetzung gesetzlicher Maßnahmen zum Auskunftersuchen für Verkehrsdaten verwendet werden (siehe Teil B dieser TR TKÜV).

Anlage X.3 Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)

Die Anlage gibt den Stand der Regelungen für die Registrierung- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur (Policy) bei Herausgabe dieser Ausgabe der TR TKÜV wieder.

Das aktuelle Dokument steht auf der Homepage der Bundesnetzagentur im Sachgebiet Telekommunikation unter dem Stichwort Technische Regulierung Telekommunikation / Techn. Umsetzung von Überwachungsmaßnahmen zum Download bereit.

Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), Referat IS 16 (Policy) zur TR TKÜV

~~Version 1.7~~Ausgabe 1.8
~~März 2015~~September 2016

---

1 Allgemeines

1.1 Einleitung

Diese Policy enthält die Regelungen der Registrierungs- und Zertifizierungsinstanz der Bundesnetzagentur, Referat IS 16, (TKÜV-CA) zur Teilnahme am Virtual Private Network ´TKÜV-VPN´ und die von den Teilnetzbetreibern für die Verwaltung der Public-Key-Infrastruktur TKÜV-PKI bereitzustellenden Daten sowie eine Beschreibung des Gesamtprozesses.

Die Regelungen sind für die am Verfahren teilnehmenden berechtigten Stellen (bSn) und die nach § 110 TKG oder § 113 TKG Verpflichteten als Teilnetzbetreiber des VPN bindend.

1.2 Identität der Registrierungs- und Zertifizierungsinstanz TKÜV-CA

Adresse: Bundesnetzagentur
Referat IS 16
Canisiusstraße 21
55122 Mainz
E-Mail: is16.postfach@bnetza.de

Hinweis zur E-Mail-Versendung: Bei der Versendung vertrauenswürdiger Daten (z.B. → Antrag VPN-Teilnahme) per E-Mail ist die Verschlüsselungssoftware PGP zu verwenden.

1.3 Allgemeine Informationsdienste der TKÜV-CA

Auf der Internetseite der Bundesnetzagentur www.bundesnetzagentur.de/tku werden weitere Informationen und Vorgaben der TKÜV-CA bereitgehalten.

1.4 Gültigkeit dieses Dokuments

Dieses Dokument ist die Ausgabe ~~1.7~~1.8 und hat Gültigkeit für den Betrieb des TKÜV-VPN bis auf Widerruf bzw. bis zur Veröffentlichung einer neuen Ausgabe. Informationen zur Gültigkeit dieses Dokuments werden in den allgemeinen Informationsdiensten der TKÜV-CA unter der o.g. Internetadresse bekannt gegeben.

2 Leistungen der TKÜV-CA

2.1 Erzeugung der Zertifikate, Verwaltung der CA

Die TKÜV-CA erzeugt und verwaltet die Zertifikate zur Teilnahme am TKÜV-VPN bzw. zur Ermöglichung der gesicherten Übermittlung zwischen Verpflichteten und berechtigten Stellen. Hierzu registriert sie die jeweiligen Teilnehmer, erzeugt pro Teilnehmer die zur Authentifizierung der Systeme notwendigen kryptographischen Schlüssel und zertifiziert diese mit ihrem eigenen CA-Schlüssel. Die so erstellten Zertifikate werden auf SmartCards gespeichert, die von den jeweiligen Teilnehmern zur Verfügung gestellt werden.

Weiterhin erstellt und pflegt die TKÜV-CA die Access Control List (ACL) auf der Grundlage der durch die Teilnehmer bereitzustellenden Daten und stellt diese für die Kryptoboxen zur Nutzung über einen LDAP-Verzeichnisdienst zur Verfügung. Um etwaige lokale Router zu administrieren, werden die hierzu notwendigen IP-Adressen der ACL den Teilnetzbetreibern auf Wunsch zur Verfügung gestellt.

Zur Überprüfung der Sicherheitsbeziehungen bzw. der eingesetzten Kryptoboxen betreibt die TKÜV-CA eine Testgegenstelle, die unter Berücksichtigung der normalen Ausfallmöglichkeit bereitsteht. Eine Überprüfung der Sicherheitsbeziehungen zwischen bSn und Verpflichteten durch die Bundesnetzagentur ist systembedingt nicht möglich.

2.2 Sicherheit der CA-Ausstattung

Sämtliche technische Einrichtungen der TKÜV-CA, die zum Betrieb des TKÜV-VPN benötigt werden, befinden sich in besonderen zugangsgesicherten Räumlichkeiten. Für die Dienste der TKÜV-CA werden dezidierte Rechner eingesetzt; die Kommunikation der im VPN betriebenen Kryptoboxen mit dem Verzeichnisdienst und dem zugehörigen zentralen Management ist selbst durch ein kryptographisches Verfahren geschützt.

Die Erzeugung der Zertifikate und die Bearbeitung der ACL finden nach dem "Vier-Augen-Prinzip" statt.

Der Betrieb der Gerätschaften der TKÜV-CA wird durch den Support des Herstellers der Systeme unterstützt. Diese vertraglichen Vereinbarungen beziehen sich nicht auf die bei den bSn und den Verpflichteten eingesetzten Systeme.

3 Anforderungen an die Teilnehmer

Die Teilnehmer an dem TKÜV-VPN im Sinne dieser Policy sind die bSn und die Verpflichteten mit ihren jeweiligen Teilnetzen.

Die Teilnehmer benennen der TKÜV-CA je einen CA-Verantwortlichen und ggf. Vertreter, die als Ansprechpartner für die jeweiligen Teilnetze gelten und insbesondere für die Sicherheit verantwortlich sind.

In dringenden Fällen erhalten die CA-Verantwortlichen vom CA-Administrator notwendige Informationen telefonisch, per E-Mail oder auf dem Postweg. Die kurzfristige Abfrage dieser Nachrichten muss sichergestellt sein.

Folgende Anforderungen werden an die CA-Verantwortlichen und deren Vertreter gestellt:

- Die von der TKÜV-CA beschriebenen SmartCards müssen entsprechend der üblichen Sorgfalt gegen Missbrauch durch Unbefugte geschützt sein und dürfen nur an die mit dem Betrieb bzw. der Administrierung der Kryptoboxen betrauten Personen weitergegeben werden.
- Auf Aufforderung, z.B. bei nachträglich bekannten Sicherheitsmängeln, sind die SmartCards zur Löschung der Inhaltsdaten der TKÜV-CA zurückzugeben.
- Liegt ein Grund zur Sperrung des Zertifikates (z.B. Betriebseinstellung, Verlust der SmartCard, Missbrauch) vor, ist dies unverzüglich der TKÜV-CA mitzuteilen, damit dort die notwendigen Folgeschritte (z.B. Sperrung im Verzeichnisdienst, Widerruf des Zertifikates) eingeleitet werden können.
- Im Übrigen gelten die Anforderungen der TKÜV, insbesondere § 15 TKÜV (Verschwiegenheit).

4 Regeln für die Registrierung

Für die Registrierung werden unter der Internetadresse der TKÜV-CA entsprechende Hinweise sowie ein Formular für die Registrierung und die IP-Konfiguration der Kryptoboxen bereitgehalten (→ Antrag VPN-Teilnahme).

4.1 Registrierung der berechtigten Stellen

Aufgrund der eindeutigen Identifizierbarkeit der jeweiligen berechtigten Stelle wird auf eine persönliche Identitätsprüfung verzichtet. Ein von der berechtigten Stelle zu benennender CA-Verantwortlicher beantragt die Registrierung bzw. die Zusendung einer SmartCard bei der TKÜV-CA per E-Mail und in schriftlicher Form mit allen bereitzustellenden Daten.

Bei einer Neuaufnahme, einem Wechsel oder Wegfall der Person des CA-Verantwortlichen bzw. der Vertreter ist die TKÜV-CA unverzüglich zu unterrichten (→ Antrag VPN-Teilnahme); ein Austausch der SmartCard ist damit nicht verbunden.

4.2 Registrierung der Verpflichteten

Bei den Verpflichteten erfolgt die Registrierung in jedem Fall durch eine persönliche Identitätsprüfung anhand eines vorgelegten gültigen Personalausweises oder Reisepasses.

Als CA-Verantwortliche bzw. Vertreter sollen von den Unternehmensverantwortlichen vorrangig die Personen benannt werden, die mit der organisatorischen Gestaltung der zur Umsetzung von Überwachungsmaßnahmen vorgesehenen technischen Einrichtungen betraut sind, z.B. die Personen, die nach § 19 TKÜV benannt werden müssen oder Personen, die mit Administrator-Aufgaben befasst sind.

Der CA-Verantwortliche beantragt die Registrierung bzw. die Zusendung einer SmartCard bei der TKÜV-CA per E-Mail und in schriftlicher Form (→ Antrag VPN-Teilnahme) mit allen bereitzustellenden Daten für die zu registrierenden Personen.

Die Registrierung erfolgt i.d.R. bei der TKÜV-CA.

Bei einem Wechsel einer registrierten Person eines Verpflichteten wird eine Neu-Registrierung notwendig. Der Wegfall einer registrierten Person oder eine Umfirmierung des Verpflichteten ist der TKÜV-CA unverzüglich mitzuteilen (→ Antrag VPN-Teilnahme); ein Austausch der SmartCard ist damit nicht verbunden.

5 Regeln für die Zertifizierung

Die TKÜV-CA erstellt nur Zertifikate für das Gesamtverfahren TKÜV-VPN.

Für die Zertifizierung werden unter der Internetadresse der TKÜV-CA entsprechende Hinweise und Formulare zur Zertifizierung bereitgehalten.

Die Zertifikate werden mit einer~~, technisch bedingten, maximalen~~ Lebensdauer von ~~10~~ 4 Jahren eingerichtet, das ausgestellte Benutzerzertifikat ist an eine einzelne SmartCard gebunden.

5.1 Bereitzustellende Daten

Die Teilnehmer stellen im Rahmen der Zertifizierung (→ Antrag VPN-Teilnahme) die grundsätzlichen Daten für die Erzeugung der X.509-Zertifikate und für die Erstellung/Ergänzung der ACL im Verzeichnisdienst bereit. Die daraufhin im Detail folgende Festlegung trifft die TKÜV-CA eigenverantwortlich. Die bereitgestellten Daten werden sicher verwahrt.

Das Namensschema wird durch die TKÜV-CA vorgegeben. Andere Namenskonventionen müssen aufgrund des geschlossenen VPN nicht beachtet werden.

A. Daten für die X.509-Zertifikate
(Festlegung durch TKÜV-CA)

Die bei dem Verfahren eingesetzten X.509v3-Zertifikate stellen die Verbindung zwischen der Identität der Teilnehmer in der TKÜV-PKI in Form eines X.500-Distinguished Name (DN) und einem public key her, die durch die digitale Signatur der

TKÜV-CA beglaubigt wird. Der DN wird als subject innerhalb des Zertifikates mit dem public key verknüpft. Das Format wird in der nachfolgenden Tabelle dargestellt.

Tabelle ´Format des X.500-Distinguished Name (DN)´

Feld	Bedeutung	Festlegung
C	Land (Country)	DE
SP	State of Province Name (Bundesland)	. [1)]
L	Locality Name (Ort)	. [1)]
O	Organization Name (Organisation)	regtp_sina
OU	Organizational Unit Name (Abteilung)	ggf. weitere Unterteilung (neben CN)
CN	Common Name (Name)	Name der bS bzw. des Verpflichteten (z.B. "LKA_Stuttgart_1")
Email	E-Mail-Adresse der Identität	zur einfacheren Namensverwaltung (wird automatisch aus den Angaben abgeleitet und hat die Form: CN@[OU].O.C)

[1)] Bei dem Eintrag "." bleibt das Feld frei.

Der Distinguished Name entspricht dem User-Name der Kryptobox, der auf dem Display der Kryptobox abgerufen werden kann.

Beispiel: C: DE, O: regtp_sina, CN: LKA_Stuttgart_1, → LKA_Stuttgart_1@regtp_sina.de

Tabelle ´Struktur des X.509v3-Zertifikates´

Feld	Bedeutung	Festlegung
version	Version des X.509-Zertifikates	3
serial number	einmalige Nummer je Zertifikat	laufende Nummer
signature	verwendeter Algorithmus der Signierung	
issuer	Distinguished Name der TKÜV-CA	s.o.
validity	Gültigkeitsdauer	
subject Name	Distinguished Name der bS bzw. des Verpflichteten	
subject PublicKeyInfo	public key des Inhabers (subject Name)	
unique Identifiers		wird nicht genutzt
Extensions		
rfc822Name	Abbildung des DN auf eine E-Mail-Adresse	wird für IPSec genutzt; erfolgt automatisch

Daten für die Erstellung/Ergänzung der ACL
(Festlegung durch TKÜV-CA nach allgemeiner Vorgabe durch die Teilnehmer)

Die Access Control List (ACL) beinhaltet alle gültigen Sicherheitsbeziehungen der jeweiligen Teilnehmer und wird ausschließlich von der TKÜV-CA verwaltet.

Nach der Inbetriebnahme oder nach einem erfolgten Neustart der Kryptobox mit der durch die TKÜV-CA ausgelieferten SmartCard baut die Kryptobox automatisch eine Verbindung zum Verzeichnisdienst auf und lädt die aktuelle ACL. Die bereitgestellte ACL ist jeweils durch die TKÜV-CA signiert; die Kryptoboxen akzeptieren keine unsignierte ACL. Danach ist das System betriebsbereit.

Die für die Erstellung bzw. Ergänzung der ACL notwendigen Daten beziehen sich auf das erzeugte Zertifikat und auf die von den Teilnehmern bereitzustellenden eindeutigen IP-

Adressen zur Adressierung der Anwendung (IP-Endpoint) hinter der Kryptobox (IP-WAN und IP-Lokal).

Für die Benennung der IP-Adressen wird den Teilnetzbetreibern ein Hilfeschema mit einer Beispielkonfiguration vorgegeben (→ Antrag VPN-Teilnahme, Schaubild).

Für die Richtigkeit der Angaben sind die Teilnetzbetreiber verantwortlich; seitens der Bundesnetzagentur kann lediglich eine einfache Plausibilitätskontrolle durchgeführt werden.

Tabelle ´Notwendige öffentliche IP-Adressen zur eindeutigen Adressierung´

Feld	Bedeutung	Festlegung
IP-Router-WAN	interne IP-Adresse des (Default-) Routers zum Internet hin	erforderlich
IP-Krypto-WAN	IP-Adresse / Subnetzmaske der Kryptobox zum Internet hin	erforderlich
IP-Krypto-Lokal	IP-Adresse / Subnetzmaske der Kryptobox zum internen Netz hin	erforderlich
IP-Router-Lokal	IP-Adresse des internen Routers, um weitere Subnetze an die Box anzuschließen	optional (hängt von der Netzstruktur ab)
IP-Anwendung	IP-Adresse(n), der im Rahmen der Umsetzung der gesetzlichen Maßnahmen bereitzustellenden Systeme	erforderlich [1)]
IP-Logserver	IP-Adresse eines eigenen Log-Servers zum Empfang der Betriebs- und Audit-Logs	erforderlich [1)]

1) Für die Anbindung können private IP-Adressen genutzt werden; diese müssen dann mittels Adressübersetzung (NAT) an die öffentliche IP-Adresse der IP-Kryptobox (IP-Krypto-Lokal) angebunden werden. Das NAT seinerseits muss dann natürlich eine eindeutige IP-Adresse zur Kryptobox erhalten.

5.2 Hinweise

- **Unveränderbarkeit der Anbindung der Kryptoboxen an das Internet**

  Die genaue Anbindung der Kryptobox an das Internet (IP-Konfiguration) als teilnehmerseitiger Anteil der Sicherheitsbeziehung zum Management und LDAP-Server der TKÜV-CA sowie zum eigenen IP-Logserver wird auf der SmartCard persistent mit der Option Auto-Init gespeichert, um beim Start der Kryptobox den Download der ACL bzw. das Melden etwaiger Fehler zu ermöglichen. Bei Änderungen wird über das Antragsverfahren (→ Antrag VPN-Teilnahme) die Ausstellung einer neuen SmartCard erforderlich.
  Bei Änderungen der eigentlichen Anwendung (IP-Anwendung, Applikation), die keine Auswirkungen auf die IP-Konfiguration haben, ist die Ausstellung einer neuen SmartCard nicht notwendig.

- **Freigabe nur definierter Hosts (Applikationen) hinter der Kryptobox**

  Neben den Sicherheitsbeziehungen zwischen der Kryptobox und dem Management sowie dem LDAP-Server der TKÜV-CA und dem eigenen IP-Logserver werden nur genau definierte Hosts (Applikationen) als Sicherheitsbeziehungen innerhalb der ACL definiert; die Freigabe eines ganzen Subnetzes ist möglich. Die TKÜV-CA behält sich jedoch vor, die Anzahl einzelner Sicherheitsbeziehungen oder die Größe des Subnetzes nach eigenem Ermessen zu beschränken. Die Sicherheitsbeziehungen zwischen den Hosts der Verpflichteten und der bSn sind immer wechselseitig.

- **Einsatz von Routern, Paketfiltern, Firewalls etc.**

  Bei dem Einsatz von Routern oder Netzelementen mit Paketfilter- oder Firewall-Funktionen auf der internen Seite zwischen Kryptobox und Host in den Teilnetzen ist sicherzustellen, dass - wenn notwendig - es durch deren Administrierung bei der Umsetzung einer Anordnung zu keiner Verzögerung oder Verhinderung kommt. Sofern solche Netzelemente für die IP-Konfiguration von Bedeutung sind, sind sie zu benennen.

- **Bereitstellung der IP-Adressen der Partner**
  Um etwaige Netzelemente für das Routing administrieren zu können, stellt die TKÜV-CA Listen der notwendigen IP-Adressen auf einem durch die TKÜV-CA betriebenen und durch eine Kryptobox geschützten FTP-Server zur Verfügung. Die Betreiber der Teilnetze erhalten auf Wunsch eine Zugriffsberechtigung; der Abruf und die Einpflege dieser Liste liegt in der Verantwortung der Betreiber der Teilnetze, die Inhalte der Listen sind vertraulich zu behandeln.

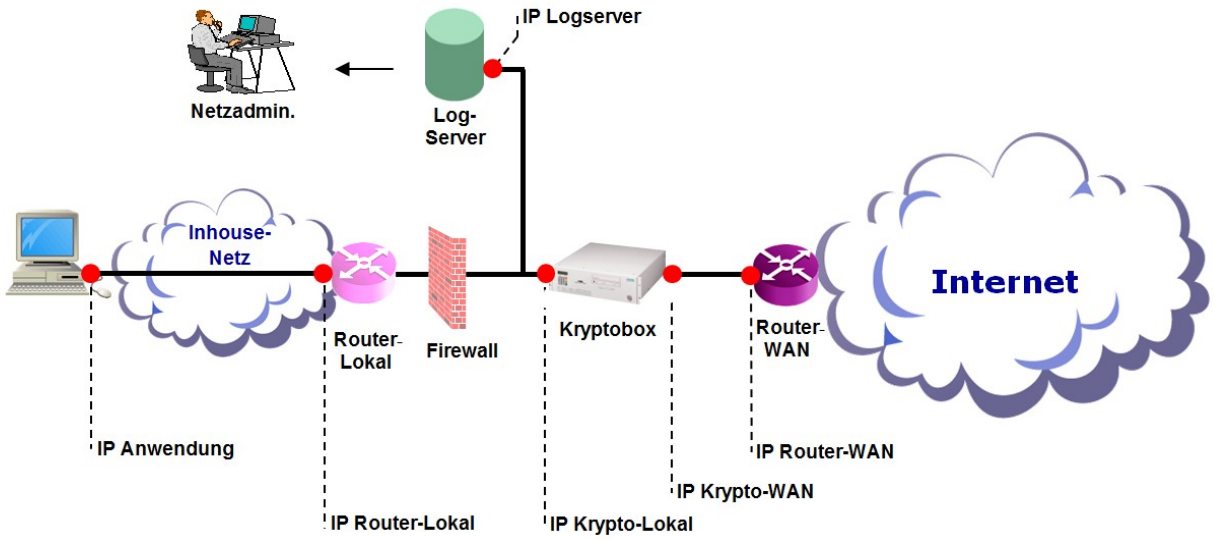
5.3 Test der Sicherheitsbeziehungen bzw. der eingesetzten Kryptoboxen

Nach Inbetriebnahme des Teilnetzes ist zur Sicherstellung der Funktion ein Test mit der Testanlage der TKÜV-CA für die bSn und die Verpflichteten vorgesehen. Dieser Test dient der Überprüfung der grundsätzlichen Funktion der IP-Konfiguration sowie der zum Management und den Testsystemen eingerichteten Sicherheitsbeziehungen; er findet bei den Verpflichteten im Vorfeld der Abnahme der technischen Überwachungseinrichtung statt. Eine Überprüfung der Sicherheitsbeziehungen zwischen bSn und Verpflichteten durch die Bundesnetzagentur ist systembedingt nicht möglich.

5.4 Merkblatt zur eindeutigen Adressierung der Teilnetze

Bei Teilnahme am VPN bzw. beim Einsatz der Kryptoboxen in den Teilnetzen der Verpflichteten und der bSn ist darzulegen, wie die Forderung nach einer eindeutigen Adressierung des jeweiligen Teilnetzes erfüllt wird. Darüber hinaus sind die für das Verfahren notwendigen IP-Adressen der TKÜV-CA zu nennen. Zur Unterstützung der Teilnehmer bei der Planung wurde ein Merkblatt entwickelt, das bei den Informationsdiensten bereitsteht. Für die Vollständigkeit des Merkblattes kann aufgrund der Vielfalt technischer Lösungsmöglichkeiten keine Gewähr gegeben werden.

5.5 Beispielskizze



Skizze 1 ´Beispiel eines Teilnetzes mit eindeutigen IP-Adressen´

Ein weiteres Beispiel ist im Antrag VPN-Teilnahme enthalten.

6 Sperrung der SmartCard

Die Sperrung einer SmartCard erfolgt durch einen entsprechenden Eintrag in einer Blacklist, die an alle beteiligten Kryptoboxen übermittelt bzw. bei einem Neustart von diesen geladen wird. Der Eintrag in der Blacklist bewirkt, dass die mit dieser SmartCard ausgestattete Kryptobox von der Teilnahme am VPN ausgeschlossen wird. Identische Reservekarten sind davon ebenfalls betroffen. In der Regel erfolgt die Sperrung der Karte nach Rücksprache mit dem entsprechenden VPN-Teilnehmer. Sie kann jedoch auch bei gegebenem Anlass unmittelbar erfolgen.

Die Sperrung einer SmartCard kann zum Beispiel notwendig werden, wenn

- die ausgegebene SmartCard verloren oder kompromittiert wurde,
- ein Missbrauch vorliegt oder gegen die Vorgaben der TKÜV-CA verstoßen wird,
- Umstände vorliegen, die eine vorübergehende Stilllegung der Kryptobox erfordern.

Die VPN-Teilnehmer sind verpflichtet, einen möglichen Sperrgrund unverzüglich mitzuteilen. Je nach Sperrgrund kann eine gesperrte SmartCard auch wieder aus der Blacklist entfernt werden, so dass sie im normalen Betrieb weiter verwendet werden kann.

7 Widerruf von Zertifikaten

Der Widerruf von Zertifikaten kann nur direkt bei der TKÜV-CA durch einen Eintrag im Verzeichnisdienst erfolgen. Die VPN-Teilnehmer sind verpflichtet, einen möglichen Widerrufsgrund unverzüglich mitzuteilen.

Ein Widerruf von Zertifikaten kann zum Beispiel erforderlich werden, falls

- die ausgegebene SmartCard verloren oder kompromittiert wurde,
- Angaben zum Zertifikat ungültig sind (Wechsel der IP-Konfiguration, Einstellung des Betriebs),
- ein Missbrauch vorliegt oder gegen die Vorgaben der TKÜV-CA verstoßen wird.

Ein Widerruf eines Zertifikats erfolgt immer wenn eine SmartCard gelöscht wird.

In der Regel erfolgt der Widerruf eines Zertifikates nach Rücksprache mit dem entsprechenden VPN-Teilnehmer. Bei gegebenem Anlass kann der Widerruf jedoch auch unmittelbar erfolgen. Eine Rücknahme des Widerrufs ist nicht möglich. Für eine Wiederaufnahme des Betriebs ist die Ausstellung einer neuen SmartCard erforderlich.

8 Verteilung und Handhabung der SmartCards

Für die Konfigurations- und Authentifizierungsdaten werden SmartCards verwendet, auf denen Informationen zum Nutzer und zur Kryptobox gespeichert werden.

Entsprechende Leerkarten in der benötigten Menge sind dem Antrag VPN-Teilnahme durch den jeweiligen VPN-Teilnehmer beizufügen. Es wird grundsätzlich empfohlen, pro IP-Kryptobox eine identische Ersatzkarte anfertigen zu lassen. Die Verteilung der SmartCards durch die TKÜV-CA erfolgt persönlich oder per Postversand an den benannten Personenkreis (registrierte Personen) des jeweiligen VPN-Teilnehmers.

Die SmartCards werden standardmäßig durch eine PIN-/PUK-Kombination geschützt. Die PIN wird durch die TKÜV-CA auf einen Wert gesetzt, bei dem die Kryptobox nach dem Einschalten ohne PIN-Abfrage in den Betriebszustand bootet. Die PIN kann zwar über die Tastatur der Kryptobox überschrieben werden; bei einer anderen als der eingetragenen PIN ist jedoch bei jedem Booten des Systems (Aus-/Einschalten) die manuelle Eingabe der PIN an der Kryptobox notwendig.

Eine Änderung der PIN sollte daher nicht durchgeführt werden!

9 Inhaltsdaten

Auf der SmartCard sind bei Versendung durch die TKÜV-CA die in der nachfolgenden Tabelle festgeschriebenen Festlegungen gespeichert. Dabei bedeutet:

- Spalte M (wie Manipulationsgeschützt): Die Daten, bei denen sich ein „X“ in der Spalte befinden, sind manipulationsgeschützt auf der SmartCard abgelegt.
- Stichwort IP-Adressen: Als „schwarze Seite“ bzw. als „schwarzes Netz“ ist die dem Internet zugewandte und damit unsichere, verschlüsselte Seite der Kryptobox gemeint. „Rote Seite“ bzw. „rotes Netz“ bezeichnet den im sicheren Netz liegenden, unverschlüsselten Bereich.

Stichwort	M	Festlegung / Stichwort
Public key der CA	X	
Zertifikat der CA	X	Zertifikat und public key der Zertifizierungsinstanz
Schlüsselpaar des Nutzers	X	Zertifikat, public key und private key des Nutzers
Gültigkeit der Zertifikate	X	Im Zertifikat des Nutzers codiert; ~~maximal 10~~ 4 Jahre
Parametersätze für Schlüsselaustausch		Für die Berechnung von temporären Schlüsseln zwischen den Teilnehmern notwendige kryptographische Parameter
Sicherheitsbeziehungen		Je eine Sicherheitsbeziehung zum Managementsystem und zum LDAP-Verzeichnis (notwendig für das nach Einschalten der Kryptobox initiale Herunterladen der ACL) sowie Sicherheitsbeziehungen zu den Testgegenstellen der Bundesnetzagentur. Diese Sicherheitsbeziehungen werden generell persistent gespeichert; das bedeutet, dass diese Beziehungen nicht durch Einträge der ACL überschrieben werden können. Bestandteil der Sicherheitsbeziehung sind die zu verwendenden kryptographischen Funktionen (Einwegfunktion / Verschlüsselungsalgorithmus)
PIN / PUK		Schutzmechanismus
IP-Adresse der Kryptobox (schwarze Seite)		Interface-Bezeichnung (~~grundsätzlich eth0~~ethX), IP-Adresse / Subnetz-Maske
IP-Adresse des WAN-Routers (schwarze Seite)		IP-Adresse

IP-Adresse der Kryptobox (rote Seite)		Interface-Bezeichnung (~~grundsätzlich eth1~~ethY), IP-Adresse / Subnetz-Maske
Freigaben		IP-Adressen der Freigaben
IP-Adresse des / der Syslog-Server		IP-Adresse des eigenen Syslog-Servers
IP-Adresse des / der NTP-Server		Die TKÜV-CA betreibt einen eigenen NTP-Server, dessen IP-Adresse eingetragen wird; es kann jedoch auch ein eigener NTP-Server genutzt werden
Zeitschranke		Zeitintervall für die Abfrage des NTP-Servers
IP-Adresse des Hot-Standby-Interfaces		Nur wenn genutzt: Interface-Bezeichnung (~~grundsätzlich eth2~~ethZ), IP-Adresse / Subnetz-Maske

Über das Menüsystem des in der Kryptobox integrierten Kartenlesers sind verschiedene Betriebseinstellungen ablesbar und teilweise veränderbar (PIN, Zeit); nähere Erläuterungen befinden sich im Handbuch der Kryptobox.

Beispiele:

Stichwort	**Festlegung / Stichwort**
IP Konfiguration, "schwarze Seite"	→ Interface-Bezeichnung (~~grundsätzlich eth0~~ethX) → IP-Adresse / Subnet-Maske
IP Konfiguration "rote Seite"	→ Interface-Bezeichnung (~~grundsätzlich eth1~~ethY) → IP-Adresse / Subnet-Maske
LDAP-Server	→ IP-Adresse
Syslog-Server	→ IP-Adresse
NTP-Server	→ IP-Adresse
Identities	→ username = Distinguished Name
Versions	→ ACL-Version → Anzahl der Policies
Show/Set Time	→ Anzeige / Einstellen von Datum und Uhrzeit

10 Management der Kryptoboxen / Optionsauswahl

10.1 Architektur des Managements und der Testeinrichtungen bei der Bundesnetzagentur

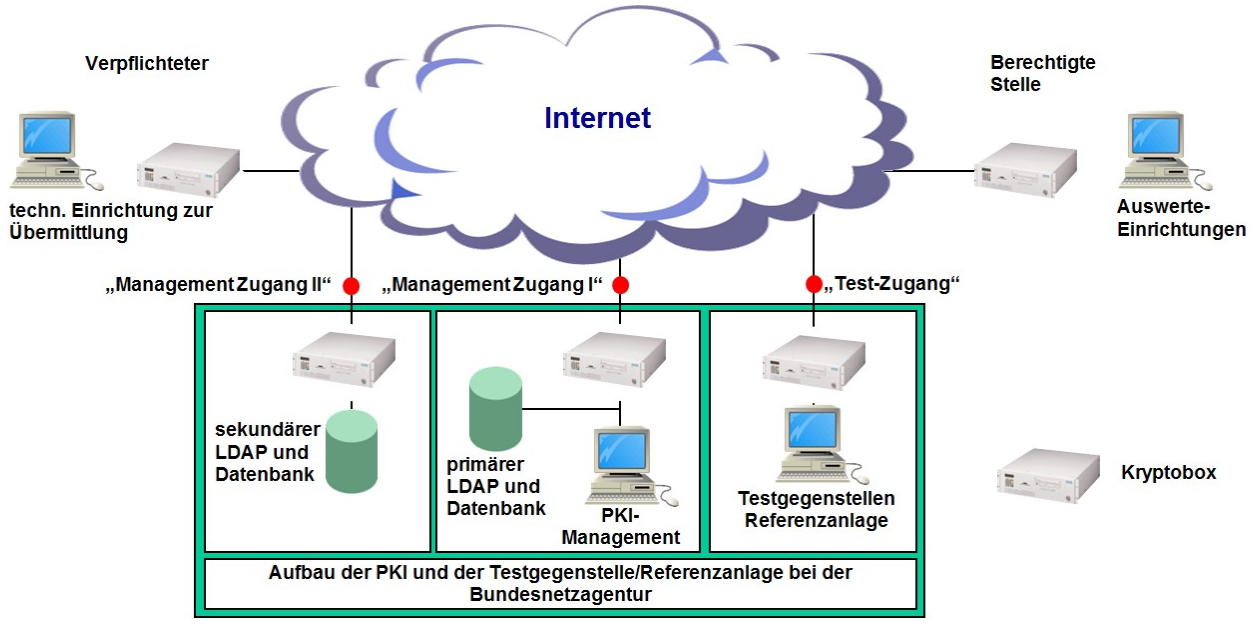
Die Architektur des gesamten Managements am Standort der TKÜV-CA für die in den Teilnetzen eingesetzten Kryptoboxen ist auf zwei Teilsysteme aufgeteilt:

- eine Managementstation zur Administrierung der Kryptoboxen, Einrichten der Sicherheitsbeziehungen und Erstellen der SmartCards sowie
- ein Server für den Verzeichnisdienst (LDAP) und einer allgemeinen Datenbank.

Die beiden Teilsysteme werden über Kryptoboxen mit dem Internet verbunden. Das gesamte Management ist aus Redundanzgründen gedoppelt.

Zu den Teilsystemen muss je eine Sicherheitsbeziehung für jede Kryptobox (nicht zu den dahinter liegenden Hosts) der Teilnetze der bSn bzw. der Verpflichteten auf der SmartCard fest eingerichtet werden. Das Managementsystem muss die Kryptoboxen erreichen, um ein ACL-Update zu ermöglichen und die Kryptoboxen müssen den Server erreichen, um die aktuelle ACL laden zu können.

Sämtliche Sicherheitsbeziehungen werden durch die TKÜV-CA eingerichtet. Die Sicherheitsbeziehungen zu den Teilsystemen des Managementsystems müssen auf den SmartCards fest gespeichert werden; die Sicherheitsbeziehungen der Hosts der Verpflichteten zu den Hosts der bSn werden in der ACL des Verzeichnisdienstes eingetragen, die dann automatisch oder manuell durch die TKÜV-CA in die Kryptoboxen geladen wird.



Skizze 2 ´Architektur des Management und Testeinrichtungen bei der Bundesnetzagentur´

Die Testeinrichtung (Referenzanlage) der Bundesnetzagentur dient zur Abnahme nach § 110 TKG oder §113 TKG ~~und~~ sowie zum Funktionstest der Kryptoboxen der bSn und der Verpflichteten nach Inbetriebnahme der Kryptoboxen. Eine Funktionsprüfung der zwischen Verpflichteten und bSn per ACL definierten Verbindungen durch die Bundesnetzagentur kann systembedingt nicht durchgeführt werden. Den Teilnehmern bietet sich jedoch die Möglichkeit nach § 23 TKÜV an.

11 Optionsauswahl / Festlegungen

Das Managementsystem erlaubt zur Konfiguration der Kryptoboxen und der Sicherheitsbeziehungen verschiedene Optionen, die vor der Erstellung der SmartCards festgelegt werden müssen. Diese Optionen sind nachfolgend dargestellt.

11.1 Log-Server

Da jeder Teilnetzbetreiber für Planung, Betrieb, Wartung und Entstörung der Kryptoboxen verantwortlich ist, müssen jeweils eigene Log-Server betrieben werden. Die Bundesnetzagentur stellt keine Log-Server für die Teilnehmer zur Verfügung; sie erhält auch keinen Zugriff auf die teilnehmerseitigen Log-Server.

Die eingesetzten Kryptoboxen besitzen keine lokalen Massenspeicher wie Festplatten oder Floppylaufwerke. Ereignisprotokolle können somit nicht lokal abgelegt werden. Da diese aber für die Überwachung der Kryptoboxen und des Netzwerks erforderlich sind, müssen Log-Server eingerichtet werden. Die IP-Adresse des Log-Servers sowie die Verbindung zwischen dem einzelnen Kryptoboxen und zugehörigem Log-Server werden auf der SmartCard persistent gespeichert. Als Protokoll wird generell UDP über Port 514 verwendet.

Es können mehrere SYSLOG-Server pro Kryptobox eingerichtet werden, die Logdaten werden dann an alle Log-Server gesendet.

~~Da jeder Teilnetzbetreiber für Planung, Betrieb, Wartung und Entstörung der Kryptoboxen verantwortlich ist, müssen jeweils eigene Log-Server betrieben werden. Die Bundesnetzagentur stellt keine Log-Server für die Teilnehmer zur Verfügung; sie erhält auch keinen Zugriff auf die teilnehmerseitigen Log-Server. Als Protokoll wird generell UDP 514 verwendet.~~

~~Zur besseren Auswertung der Syslog-Meldungen wird das von Secunet erhältliche Dokument „Logmeldungen“ empfohlen. Dieses enthält eine Übersicht der „Log-IDs“ welche ab einer Software-Version 2.x.x bei den SINA-Boxen zum Einsatz kommen.~~

~~Es gelten zudem die Hinweise aus Abschnitt 5.~~

11.2 Heartbeat

Zusätzlich zum Logserver kann ein Zeitintervall angegeben werden, nach dem von einer Kryptobox eine Meldung an den/die Logserver gesendet wird, um den Betrieb zu signalisieren, auch wenn keine weiteren Aktivitäten zu protokollieren sind. Mit dieser Information werden bestimmte Systemzustände übertragen, z. B. Interfacestatistiken und Uptime. Ist kein Wert gesetzt, wird kein Heartbeat geliefert. Normale Aktivitäten werden jedoch unabhängig von dieser Einstellung immer protokolliert. Die Heartbeat-Einstellung gilt für alle eingetragenen Log-Server.

Innerhalb des Antragsverfahrens (→ Antrag VPN-Teilnahme, Optionsblatt) können die jeweiligen Teilnetzbetreiber angeben, wie diese Funktion genutzt werden soll.

11.3 NTP-Server

Der NTP-Server stellt den Zeitdienst innerhalb der PKI bereit. Mittels der dort abzufragenden Zeit (inkl. Datum) stellt die Kryptobox fest, ob ein Zertifikat noch gültig ist. Hat eine Box noch keinen Zugang zu einem NTP-Server, weil diese Verbindung erst etabliert werden muss, so wird die lokale Zeit der auf dem Board befindlichen Systemuhr zum Vergleich hinzugezogen. Nach erfolgreicher Verbindung zu einem NTP-Server wird ebenfalls die Systemuhr der Kryptobox mit dessen Zeit synchronisiert.

Die Bundesnetzagentur stellt über das Managementsystem NTP-Server ausschließlich für die Kryptoboxen bereit; die erforderlichen Sicherheitsbeziehungen werden persistent auf der SmartCard eingetragen. Referenzzeit ist UTC, die aus der amtlichen Zeit der Bundesrepublik Deutschland abgeleitet wird. Optional kann ein teilnehmereigener NTP-Server eingetragen werden.

Die Einrichtung mehrerer NTP-Server pro Kryptobox ist möglich. Die Abfrage erfolgt dann entsprechend der auf der SmartCard eingetragenen Reihenfolge.

Die Abfrage eines NTP bewirkt einen Eintrag im Syslog.

11.4 Bereitstellung der IP-Adressen der Partner-Teilnetze

Um gegebenenfalls Netzelemente für Routing/Filterung administrieren zu können, stellt die TKÜV-CA eine Liste der notwendigen IP-Adressen auf einem eigenen, durch eine Kryptobox geschützten, FTP-Server zur Verfügung. Die Betreiber der Teilnetze erhalten auf Wunsch eine Zugriffsberechtigung; der Abruf dieser Liste liegt in der Verantwortung der Betreiber der Teilnetze. Die Aktualisierung der Liste erfolgt nur bei Bedarf.

11.5 Hot-Standby (HSB)

Im Hot-Standby-Modus werden zwei Kryptoboxen als Cluster installiert. Ein Gerät ist aktiv (Master oder Sys1), das zweite Gerät (Slave oder Sys2~~bzw. Backup~~) übernimmt beim Ausfall des ersten dessen Funktion. Für diese Betriebsart sind speziell vorbereitete Smartcards erforderlich.

11.6 Software-Version SINA-Box

Derzeit werden als Kryptoboxen ausschließlich SINA-Boxen des Herstellers Secunet verwendet. Als SINA-Boxen-SW sind nur noch die Versionen 2.2.8.x und 2.2.10.x zulässig ~~Die verwendete Software-Version einer SINA-Box sollte möglichst einer aktuellen, von Secunet herausgegebenen Version entsprechen. Als älteste noch einsetzbare SINA-Box-Software gilt die Version 2.2.0~~ Diese ~~Mindestversion~~ Vorgabe muss bis spätestens ~~bis zum 30.06.2016~~31.03.2017 umgesetzt sein. ~~eingesetzt werden.~~

Diese Festlegung soll u.a. die Systemkompatibilität bei zukünftigen Updates am SINA-Management gewährleisten, aber auch den generellen Support von Secunet bezüglich den SINA-Boxen/-Software sicherstellen. Des Weiteren wird von Secunet erst ab der ~~Software~~SW-Version 2.x.x.x mit „Log-IDs“ gearbeitet, welche die Auswertung von Syslog-Meldungen erheblich erleichtern.

Der Einsatz einer SINA-Boxen-SW der Version 3.x.x.x ist derzeit noch nicht möglich.

11.7 Smartcards

Für aktuelle und zukünftige Anträge sind nur noch Smartcards mit dem Betriebssystem „STARCOS“ zu verwenden.

12 Mitgeltende Dokumente

Mitgeltende Dokumente in ihrer jeweils aktuellen Fassung sind:

- Telekommunikationsgesetz (TKG)
- Telekommunikations-Überwachungsverordnung (TKÜV)
- Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV)
- Antrag VPN_Teilnahme

Anlage X.4 Tabelle der anwendbaren ETSI- und 3GPP-Standards bzw. Spezifikationen sowie der ASN.1-Module

Auf der Grundlage des § 11 Satz 5 TKÜV informiert die Bundesnetzagentur auf ihrer Homepage der Bundesnetzagentur im Sachgebiet Telekommunikation unter dem Stichwort Technische Regulierung Telekommunikation / Techn. Umsetzung von Überwachungsmaßnahmen über die anwendbaren Ausgabestände der nach TR TKÜV festgelegten ETSI- und 3GPP-Standards und Spezifikation.

Wesentlicher Bestandteil ist dabei die Nennung der anwendbaren ASN.1-Module.

Grundsätzlich sind eventuelle vorhandene Syntaxfehler in den ASN.1-Modulen zu berichtigen und es ist auf die Verwendung des richtigen Object Identifiers (OID) bzw. der richtigen Versionsnummer zu achten. Zudem sind Versionen der Module von der Verwendung ausgeschlossen, die nicht rückwärts-kompatibel zu den anderen Versionen sind.

Die nachfolgende Tabelle enthält diese Informationen bei Herausgabe dieser Ausgabe.

Anwendbare ASN.1 Module (neuere Versionen als die angegebenen können grundsätzlich genutzt werden)	**Ausgabe des Standards bzw. der Spezifikation**	**Anforderung bzw. Hinweis zur Anwendung**
ETSI ES 201 671, TS 101 671 (Anlage C)		
Hier werden die Versionen der Module aufgenommen, die über einen OID verfügen sowie die älteren Versionen, die bereits in den Netzen implementiert und deren Konzepten zugestimmt wurden.		
HI2Operations	Version 10	In dieser Version befindet sich ab der Ausgabe 3.2.1 der Spezifikation ein Fehler, der die Kompatibilität aufhebt. Diese Version darf daher nur bis zur Ausgabe 3.1.1. verwendet werden.
HI2Operations	Version 11	In dieser Version befindet sich ein Fehler, der die Kompatibilität aufhebt. Diese Version darf daher nicht verwendet werden. Mit der Ausgabe 3.6.1 der Spezifikation ist der Fehler in der dortigen Version 12 behoben.
3GPP TS 33.108 (Anlage D)		
Hier werden die Versionen der Module aufgenommen, die über einen OID verfügen sowie die älteren Versionen, die bereits in den Netzen implementiert und deren Konzepten zugestimmt wurden.		
ETSI TS 102 232-01 (Anlage F.3 und G)		
LI-PS-PDU, version 4	Version 1.4.1	
ETSI TS 102 232-02 (Anlage F.3)		
EmailPDU, version 3	Version 2.1.1	
ETSI TS 102 232-03 (Anlage G)		
IPAccessPDU, version 4	Version 1.6.1	
ETSI TS 102 232-04 (Anlage G)		
L2AccessPDU, version 3	Version 1.3.1	
ETSI TS 101 909-20-2 (Anlage G)		
PCESP, version-4(4) TS101909202, interceptVersion (0)	Version 1.1.2	~~Die Originalmodule enthalten Syntaxfehler; Anlage X.6 enthält berichtigte Versionen dieser Module~~
ETSI TS 102 232-05 (Anlage H.1)		
IPMultimediaPDU, version 1	Version 2.1.1	
ETSI TS 102 232-06 (Anlage H.2)		
PstnIsdnPDU, version 1	Version 2.1.1	
ETSI TS 101 909-20-1 (Anlage H.3)		
TS101909201, interceptVersion (0)	Version 2.1.1	~~Die Originalmodule enthalten Syntaxfehler; Anlage X.6 enthält berichtigte Versionen dieser Module~~
ETSI TS 102 657 (Teil B)		

RDMessage, version9	Version 1.9.1	

Anlage X.5 Checkliste zu den sonstigen Anforderungen nach TKÜV bei der Umsetzung von Überwachungsmaßnahmen

Die TKÜV nennt u.a. grundsätzliche Anforderungen zur Gestaltung der technischen Einrichtungen sowie zur organisatorischen Umsetzung bezüglich Überwachungsmaßnahmen. Die folgende Checkliste soll die Verpflichteten bei der Implementierung unterstützen. Ohne weitere Erläuterung beziehen sich die Verweise in der Tabelle auf die Paragraphen der TKÜV:

A	**Grundsätzliche Anforderungen, Schutzanforderungen**		
Nr.	*TKÜV*	*Stichwort zur Anforderung*	*Erläuterungen*
A.1	§ 4 Abs. 1	Nichtüberwachung, wenn sich das Endgerät im Ausland befindet und die TKAnl dies erkennt mit Ausnahme von Um- und Weiterleitungen ins Inland.	Forderung gilt nicht bei Anordnungen entsprechend § 4 Abs. 2 ("Auslandskopf-Überwachung")
A.2	§ 5 Abs. 1	Vollständige Überwachung der Telekommunikation der zu überwachenden Kennung inkl. der Telekommunikation, die der Steuerung von Betriebsmöglichkeiten dient (z.B. über den Anschluss, per Servicerufnummer oder Webzugriff)	
A.3	§ 5 Abs. 1	Keine Überwachung der Telekommunikation, die unter anderen Kennungen abgewickelt wird	
A.4	§ 5 Abs. 4	Nichtfeststellbarkeit von Überwachungsmaßnahmen	
A.5	§ 5 Abs. 5	Berichten der Aktivierung bzw. Deaktivierung von Maßnahmen (z.B. per Ereignisdatensatz)	
A.6	§ 5 Abs. 6	Rechtzeitiges Erkennen und Beseitigen von Engpässen der Administrierungsfunktion sowie der Ausleitungskapazitäten bei der Realisierung von Überwachungsmaßnahmen	Empfehlung: Einhaltung der Richtwerte bei der Dimensionierung nach Abschnitt 3.2
A.7	§ 8 Abs. 2 Nr. 1	Zugriff auf die Überwachungsfunktion nur durch den Verpflichteten oder dessen Erfüllungsgehilfen; Fernzugriff nur über die Überwachungseinrichtung	kein direkter Zugriff auf die Überwachungsfunktion der Telekommunikationsanlage
A.8	§ 8 Abs. 2 Nr. 7b	Übermittlung der Überwachungskopie grundsätzlich unmittelbar nach dem Erkennen einer zu überwachenden Telekommunikation	
A.9	§ 8 Abs. 3	Eventuelle Kodierungen zur Verschlüsselung und/oder Komprimierung des Telekommunikationsinhaltes müssen bei der Überwachungskopie entfernt werden	
A.10	§ 14 Abs. 1	Schutz gegen unbefugte Inanspruchnahme der Überwachungsfunktion; Schutz von Übertragungsstrecken (Zugangskennung, Verschlüsselung etc.)	
A.11	§ 6 Abs. 3	Überwachung auf Grund der in Abschnitt 6 der TR TKÜV genannten Kennungen.	
A.12	§ 6 Abs. 4	Möglichkeit der gleichzeitigen Überwachung derselben Kennung durch verschiedene bSn	
A.13	§ 7 Abs. 3	Einrichten einer Überwachungsmaßnahme, zur ausschließlichen Übermittlung der Ereignisdaten ohne den Telekommunikationsinhalt (IRI Only)	
A.14	§ 9 Abs. 1	Möglichkeit der Administrierung gesonderter Zielanschlüsse der berechtigten Stelle für die Ausleitung der Telekommunikation der einer Kennung zugeordneten Speichereinrichtung; ggf. auch getrennt nach Diensten	

B	**Entgegennahme und Umsetzung der Anordnung, Rückfragen**		
Nr.	*TKÜV*	*Stichwort zur Anforderung*	*Erläuterungen*
B.1	§ 12 Abs. 1	Nennung einer im Inland gelegenen Stelle für Benachrichtigung und Entgegennahme	
B.2	§ 6 Abs. 1	Unverzügliche Umsetzung einer Überwachungsmaßnahme nach Entgegennahme der Anordnung	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.3	§ 10	Nachträgliche Übermittlung der Ereignisdaten bei Übermittlungshindernissen; eine Speicherung der Überwachungskopie ist nicht zulässig	
B.4	§ 12 Abs. 1	Allzeit telefonische Erreichbarkeit zur Mitteilung über das Vorliegen einer Anordnung und deren Dringlichkeit	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.5	§ 12 Abs. 1	Entgegennahme der Anordnung - innerhalb der Geschäftszeiten: jederzeit - außerhalb der Geschäftszeiten: unverzüglich, jedoch spätestens sechs Stunden nach der Benachrichtigung	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.6	§ 12 Abs. 2	Bei der Umsetzung einer per Telefax übermittelten Anordnung muss die Frist zur Vorlage des Originals beachtet werden	
B.7	§ 12 Abs. 3	Allzeit telefonische Erreichbarkeit für Rückfragen der berechtigten Stelle durch sachkundiges Personal	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.8	§ 12 Abs. 3	Falls die unmittelbare Klärung der Rückfrage nicht möglich ist, Information der berechtigten Stelle zur Klärung bzw. des Sachstandes - innerhalb der Geschäftszeiten: unverzüglich - außerhalb der Geschäftszeiten: innerhalb von sechs Stunden	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.9	§ 16 Abs. 1	Automatische und lückenlose Protokollierung der Operatoreingaben: - Kennzeichnung der Überwachungsmaßnahme - tatsächlich eingegebene Kennung (target) - Beginn- und Endezeitpunkt der Maßnahme - Ausleiteadressen der berechtigten Stelle - Identifikationsmerkmal des Operators - Datum und Zeitpunkt der jeweiligen Eingabe	
B.10	§ 17 Abs. 4	Sortiermöglichkeit der Protokolldaten nach betroffener Kennung und Entstehungszeitpunkt	Administriert ein Erfüllungsgehilfe für mehrere Verpflichtete, so muss diese Sortierung separiert erfolgen können (Mandantenfähigkeit)
B.11	§ 16 Abs. 2 Nr. 1-2	Aufgabentrennung bei den Zugriffsrechten und der Löschfunktion: Operator: Umsetzung der Anordnungen ohne Zugriff auf die Protokolldaten, deren Löschfunktion sowie auf die Erteilung von Zugriffsrechten Supervisor: Prüft die Protokolldaten und hat Zugriff auf die Löschfunktion der Protokolldaten	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.12	$ 16 Abs. 2 Nr. 3	Protokollierung der Nutzung der Löschfunktion: - Identifikationsmerkmal des Supervisors - Datum und Zeitpunkt der jeweiligen Nutzung	

B.13	§ 16 Abs. 2 Nr. 4	(Elektronischer) Nachweis über Erteilung, Änderung oder Löschung der Zugriffsrechte für - die Operator-Funktion - die Supervisor-Funktion - die Funktion zur Verwaltung der Zugriffsrechte für Operator und Supervisor	

B	**Entgegennahme und Umsetzung der Anordnung, Rückfragen**		
Nr.	*TKÜV*	*Stichwort zur Anforderung*	*Erläuterungen*
B.14	§ 17 Abs. 1	Grundsätzlich sind mindestens 20 Prozent der Protokolldaten zu prüfen. Bei Eingaben nach § 23 und in Fällen, in denen Tatsachen den Verdacht einer Unregelmäßigkeit begründen, sind alle Protokolldaten zu prüfen.	

C	**Abweichungen für Betreiber kleiner TK-Anlagen (nicht mehr als 10.000 Teilnehmer)**		
Nr.	*TKÜV*	*Stichwort zur Anforderung*	*Erläuterungen*
C.1	§ 21 Abs. 2	Umsetzung einer Überwachungsmaßnahme innerhalb von 24 Stunden nach Benachrichtigung	
C.2	§ 21 Abs. 4	Benachrichtigung über eine Anordnung, Dringlichkeit der Umsetzung, Entgegennahme der Anordnung und Rückfragen, - innerhalb der Geschäftszeiten: jederzeit - außerhalb der Geschäftszeiten: Benachrichtigung und Dringlichkeit innerhalb von 24 Stunden; nach Benachrichtigung innerhalb von 24 Stunden Entgegennahme der Anordnung sowie von Rückfragen	

Fortschreibung

Das Verfahren zur Fortschreibung der TR TKÜV richtet sich nach den Regelungen des § 11 TKÜV, wonach die Bundesnetzagentur die erforderlichen Einzelheiten unter Beteiligung der Verbände der Verpflichteten, der bSn sowie der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen festlegt.

Grundlegende Änderungen dieser Richtlinie werden durch eine neue Ausgabenummer vor dem Punkt gekennzeichnet.

Anpassungen und Ergänzungen von bereits in einer vorhergehenden Ausgabe beschriebenen Teile der TR TKÜV werden durch eine neue Ausgabenummer nach dem Punkt gekennzeichnet.

In beiden Fällen wird auf eine neue Ausgabe der TR TKÜV im Bundesanzeiger und im Amtsblatt der Bundesnetzagentur hingewiesen.

Ausgabenübersicht

Ausgabe	Datum	Grund der Änderung
1.0	Dezember 1995	Erstausgabe der TR FÜV
2.0	April 1997	Fortschreibung gemäß Ankündigung vom Dez. 95
2.1	März 1998	1. Anforderungen für Sprachspeicher- (Voicemail-Systeme) und vergleichbare Speicher-Einrichtungen / Aufnahme einer zusätzlichen Variante für die Übermittlung der Ereignisdaten 2. Zeitbasis für die Zeitangaben in den Datensätzen 3. Redaktionelle Korrekturen
2.2	Dezember 2000	Berichtigungen der Ausgabe 2.1 1. Aktualisierung der Anlage 1 2. Anlage 3 Kennzeichnung nicht benutzter Ziffern entweder mittels hex 'F' oder mittels 'odd/even indicator und hex '0' gemäß TABLE 4-10/Q.931 3. Anpassung der Anlage 6 3.1 Übermittlungsmethode 'Eurofile' und 'Subadresse' für die Ereignisdaten wurde gestrichen 3.2 Ausleitung zu aktiven Faxeinrichtungen bei den bSn (Unterstützung der Prozeduren nach ITU-T T.30) und Verwendung des BC 'audio' und des HLC 'Facsimile')
3.0	November 2001	Aufnahme der nationalen Anforderungen zur Umsetzung des ETSI-Standards ES 201 671 V2.1.1 in Deutschland als Anlage 7
3.1	Mai 2002	Redaktionelle Anpassung der Technischen Richtlinie an die TKÜV, Änderung der Kurzbezeichnung in TR TKÜ
4.0	April 2003	1. Technische Anforderungen im Abschnitt 5.2.3 für paketvermittelnde nicht IP basierte Netze gestrichen 2. Flexible Anwendung der Übertragungsprotokolle FTAM und FTP, damit verbunden Anforderungen an die Dateinamen in Anlage 1 3. Aufnahme der Anforderungen zur sicheren Übertragung zu überwachender Telekommunikation über IP-Netze unter Verwendung von IPSec als Anhang 4 zur Anlage 7 4. Anforderungen an die Paketierung von Ereignisdaten bei Realisierung nach Anlage 7 5. Aufnahme der nationalen Anforderungen zur Umsetzung der 3GPP-Spezifikation TS 33.108 in Deutschland als Anlage 8

Ausgabe	Datum	Grund der Änderung
		6. Aufnahme der nationalen Anforderungen zur Überwachung von E-Mail als Anlage 9
4.1	November 2004	1. Hinweis auf durchgeführte Notifizierung auf dem Titelblatt 2. In den Anlagen 7 und 8 wurde der Hinweis auf die Abstimmungen in den internationalen Gremien gestrichen. 3. Neue Version 4 des ASN.1-Moduls mit den nationalen Parametern (Anlage 7 Anhang 3) 4. Festlegung der Portnummer für TCP in Anlage 7, Punkt F.3.1.3 5. In Tabelle 1/A.5 wurde die maximale Dateilänge auf den Wert 25 erhöht 6. In Anlage 1 wurde ein Hinweis auf die Möglichkeit der Übermittlung der IRI nach TS 102 232 aufgenommen 7. In Anlage 5 wurden Festlegungen für die wichtigsten Parameter bei Nutzung von FTP getroffen. 8. In Anlage 7 Anhang 2 wird auf die Möglichkeit der Übermittlung der HI1 Notifications hingewiesen 9. Einfügen der nationalen Parameter als integraler Bestandteil des HI2-Moduls in Anlage 7 Anhang 2 10. Präzisierung der Behandlung von Logdateien in Anlage 7 Anhang 4 11. Anlage 9, Übernahme der Anforderungen auf Basis des ETSI Standards TS 102 233 12. Anlage 10, Übernahme der Anforderungen für eine IP-basierte Ausleitung auf Grundlage des ETSI-Standards TS 102 232
5.0	Dezember 2006	1. Neustrukturierung der TR TKÜ 2. Neuregelungen nach § 11 Satz 6 TKÜV (Kennungen für die Überwachung) 3. Detailregelung zum Internetzugangsweg auf der Grundlage von ETSI-Spezifikationen 4. Anpassungen im Bereich der Unified-Messaging-SystemUnified-Messaging-Systeme und für E-Mail 5. Neuregelung für die Ausleitung von SMS-Nachrichten nach der nationalen Variante (Anlage B) 6. Sonstige editorielle Korrekturen
5.1	Februar 2008	1. Anforderungen für VoIP und sonstiger Multimediadienste, die auf den Protokollen SIP, RTP bzw. H.323 und H.248 bzw. auf der IP-Cablecom-Architektur beruhen sowie für emulierte PSTN/ISDN-Dienste 2. Anpassungen im Bereich E-Mail durch die Aufnahme sämtlicher Protokolle in der ETSI-Spezifikation TS 102 232-2 3. Präzisierung im Bereich Internetzugangsweg bezüglich der darüber verteilten Dienste IP-TV, Video on demand, etc. 4. Anpassungen bezüglich der Anforderungen bei Hindernissen bei der Übermittlung der Überwachungskopie zur Empfangseinrichtung der berechtigten Stelle 5. Aufnahme des CGI-Feldes als zur Koordinaten-Angabe ergänzendes Pflichtfeld nach Anlage B 5. Sonstige editorielle Korrekturen
6.0	Dezember 2009	1. Neustrukturierung / Umbenennung 2. Erweiterung um einen optionalen Übergabepunkt für die Auskunftserteilung von Verkehrsdaten auf der Grundlage der ETSI-Spezifikation TS 102 657

Ausgabe	Datum	Grund der Änderung
		3. Optionale elektronische Übermittlung der Anordnungen 4. Sonstige editorielle Korrekturen 5. Abdruck der neuen Policy, Version 1.4 für die TKÜ-CA 6. Verfahrensbeschreibung zur Gewährleistung eindeutiger Referenznummern für TKÜ-Maßnahmen
6.1	Januar 2012	1. Anpassungen der Richtwerte, Abschnitt 3.2 2. Ergänzungen zu den möglichen Kennungen bei Überwachungen des Internetzugangsweges, Abschnitt 4.1 3. Aufnahme einer Verfahrensbeschreibung nach § 23 Abs. 1 Nr. 3 TKÜV 4. Klarstellung zur Übermittlungsverfahren FTP, Anlage A.1.2.2 5. Neue Version des nationalen ASN.1-Moduls ´Natparas`, Anlage A.3.2 6. Belegung der Calling Party Subadresse bei Auslandskopf-Überwachungen, Anlage B.3 7. Lockerungen zur Verwendung des COLP-Ckecks, Anlage B.1, C.1 und D.1 8. Festlegung auf ULICv1 für packet switched im Mobilfunk, Anlage C.1 und Anlage D.1 9. Anpassungen im Bereich E-Mail, Anlage F 10. Klarstellung bzgl. der Zuordnung verschiedener SIP-Messages zu IRI-Events sowie der Nutzung von IP-Source/Destination-Adressen, Anlage H.3.2, H.3.3 und H.3.4 11. Ergänzungen der Tabelle der anwendbaren ASN.1-Module, Anlage X.4 12. Einheitliche Vorgabe zur Verwendung von Zeitstempeln
6.2	August 2012	1. Neufassung und Zusammenlegung der Regelungen der bisherigen Teile B und C im neuen Teil B entsprechend der Verfeinerung der bereits mit Ausgabe 6.0 eingeführten neuen Schnittstellen 2. Anpassung der Anlage X.4
6.3	06. April 2016	1. Redaktionelle Überarbeitung des gesamten Dokuments 2. Anlage A: Ergänzung um Punkt 3.3 („Datenverluste“) 3. Anlage A: Ergänzende Klarstellung zu WLAN (Punkt 4.1) 4. Anlage B: Hinweis zum Ende der Nutzung von Ausleitungen nach Anlage B 5. Anlage C: Hinweis zum Ende der Nutzung von Ausleitungen nach Anlage C 6. Anlage C: Gültigkeitsbeschränkung auf ISDN/PSTN (kein Mobilfunk mehr) 7. Anlage D: Ergänzung zu Standortinformationen 8. Anlage D: Erläuterungen zu: Packet Direction, IP Adressen und Ports (Tabelle) 9. Anlage F.3.1.1: Erläuterungen zu: Network Element Identifier, Payload Direction (Tabellen) 10. Anlage G.1.1: Erläuterungen zu: Network Element Identifier, Payload Direction, (Tabellen) 11. Anlage H: Erläuterung zur Mid-Session-Interception (H.1.2), Verpflichtung zur grundsätzlich vollständigen Ausleitung der Telekommunikation (H.1.4)

Ausgabe	Datum	Grund der Änderung
		12. Anlage H.3.1: Anlage G.1.1: Erläuterungen zu: Network Element Identifier, Payload Direction, Keep-Alives und IP-Adressen (Tabellen) 13. Anlage X.3: Anpassung „Policy“ 14. Teil B: Anpassung an die aktuelle Rechtsgrundlage 15. Teil B: Weiterentwicklung der zugrunde liegenden ETSI-Spezifikation 16. Teil B: selektive Bestandsdatenabfragen 17. Teil B: Normierung / Vereinheitlichung der Netzbetreiber-Antworten für BDA und VDA 18. Teil B: flexible Nutzung der Freitextfelder 19. Teil B: Erweiterung der nationalen Module hinsichtlich der Textformerfordernis u. Einführung einer Versionierung
7.0	20.01.2017	1. Redaktionelle Überarbeitung des gesamten Dokuments 2. Teil A, Anlage A: Ergänzende Klarstellung zu WLAN (Punkt 4.1) 3. Teil A, Anlage D.1 (Tabelle C.1.1): Festlegung Portnummer 4. Teil A, Anlage F.3.1.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ 5. Teil A, Anlage F.3.1.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ 6. Teil A, Anlage F.3.1.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ 7. Teil A, Anlage G.1.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ 8. Teil A, Anlage G.1.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ 9. Teil A, Anlage G.1.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ 10. Teil A, Anlage H.1.2: Ergänzende Informationen zur Aktivierung einer ÜM bei bestehender Telekommunikationsverbindung 11. Teil A, Anlage H.3.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ 12. Teil A, Anlage H.3.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ 13. Teil A, Anlage H.3.1 (Tabelle): Hinweis Kodierungsinformationen 14. Teil A, Anlage H.3.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ 15. Teil A, Anlage H.3.2 (Tabelle 5.4): Ergänzende Hinweise zu „Events and IRI record types“ 16. Teil B: Anpassungen zu „1. Grundsätzliches“ 17. Teil B: Neue Festlegungen zu Übermittlungsverfahren 18. Teil B: Festlegungen zur Gewährleistung von Datensicherheit und Datenqualität 19. Teil B, Anlage A : Klarstellung zu verschiedenen Nutzungsverfahren, Verkehrsdaten in Echtzeit, cancel-Message, Funkzellenabfragen, Eilanordnungen, 20. Teil B, Anlage A: Aufnahme von Versionierung, Late-record, Zielwahlsuche, Kennzeichnung der Datensätze 21. Teil B, Anlage B: Festlegungen zu neuem Übermittlungsverfahren „E-Mail-ESB“

Ausgabe	Datum	Grund der Änderung
		22. Teil X, Anlage X.3: Anpassung „Policy“